

EXCERPTED EXHIBIT 1



The new browser recommended by Microsoft is hereGet speed, security and privacy with the new Microsoft Edge

No thanks [Switch now](#)

[Skip to main content](#)



Microsoft

Microsoft Services Agreement

[Microsoft Services Agreement](#)

Microsoft Services Agreement

[Home](#)

[FAQ](#)

[Microsoft Services Agreement](#)

[Microsoft Privacy Statement](#)

[Bing Suppliers Page](#)

More

All Microsoft

[Microsoft 365](#)

[Office](#)

[Windows](#)

[Surface](#)

[Xbox](#)

[Deals](#)

[Support](#)

Software

[Windows Apps](#)

[OneDrive](#)

[Outlook](#)

[Skype](#)

[OneNote](#)

[Microsoft Teams](#)

[Microsoft Edge](#)

PCs & Devices

[Computers](#)

[Shop Xbox](#)

[Accessories](#)

[VR & mixed reality](#)

[Phones](#)

Entertainment

[Xbox Game Pass Ultimate](#)

Xbox Live Gold

Xbox games

PC games

Windows digital games

Movies & TV

Business

Microsoft Azure

Microsoft Dynamics 365

Microsoft 365

Microsoft Industry

Data platform

Microsoft Advertising

Power Platform

Shop Business

Developer & IT

.NET

Visual Studio

Windows Server

Windows Dev Center

Docs

Power Apps

Other

Microsoft Rewards

Free downloads & security

Education

Virtual workshops and training

Gift cards

Licensing

View Sitemap

SearchSearch Microsoft.com

Cancel

Published: **July 1, 2019**

Effective: **August 30, 2019**

 [Print](#)

Microsoft Services Agreement

IF YOU LIVE IN (OR YOUR PRINCIPAL PLACE OF BUSINESS IS IN) THE UNITED STATES, PLEASE READ THE BINDING ARBITRATION CLAUSE AND CLASS ACTION WAIVER IN SECTION 15. IT AFFECTS HOW DISPUTES ARE RESOLVED.

These terms ("Terms") cover the use of those Microsoft consumer products, websites, and services listed [here](#) (the "Services"). You accept these Terms by creating a Microsoft account, through your use of the Services, or by continuing to use the Services after being notified of a change to these Terms.

Your Privacy

Your Privacy

Your Content

Code of Conduct

Using the Services & Support

Using Third-Party Apps and Services

Service Availability

Updates to the Services or Software, and Changes to These Terms

Software License

Payment Terms

Contracting Entity, Choice of Law, Jurisdiction

Warranties

Limitation of Liability

Service-Specific Terms

Xbox Live and Xbox Game Studios Games and Applications

Store

Microsoft Family Features

1. **Your Privacy.** Your privacy is important to us. Please read the [Microsoft Privacy Statement](#) (the "Privacy Statement") as it describes the types of data we collect from you and your devices ("Data"), how we use your Data, and the legal bases we have to process your Data. The Privacy Statement also describes how Microsoft uses your content, which is your communications with others; postings submitted by you to Microsoft via the Services; and the files, photos, documents, audio, digital works, livestreams and videos that you upload, store, broadcast or share through the Services ("Your Content"). Where processing is based on consent and to the extent permitted by law, by agreeing to these Terms, you consent to Microsoft's collection, use and disclosure of Your Content and Data as described in the Privacy Statement. In some cases, we will provide separate notice and request your consent as referenced in the Privacy Statement.

Your Content

2. **Your Content.** Many of our Services allow you to store or share Your Content or receive material from others. We don't claim ownership of Your Content. Your Content remains Your Content and you are responsible for it.

a. When you share Your Content with other people, you understand that they may be able to, on a worldwide basis, use, save, record, reproduce, broadcast, transmit, share and display (and on HealthVault delete) Your Content without compensating you. If you do not want others to have that ability, do not use the Services to share Your Content. You represent and warrant that for the duration of these Terms, you have (and will have) all the rights necessary for Your Content that is uploaded, stored, or shared on or through the Services and that the collection, use, and retention of Your Content will not violate any law or rights of others. Microsoft cannot be held responsible for Your Content or the material others upload, store or share using the Services.

b. To the extent necessary to provide the Services to you and others, to protect you and the Services, and to improve Microsoft products and services, you grant to Microsoft a worldwide and royalty-free intellectual property license to use Your Content, for example, to make copies of, retain, transmit, reformat, display, and distribute via communication tools Your Content on the Services. If you publish Your Content in areas of the Service where it is available broadly online without restrictions, Your Content may appear in demonstrations or materials that promote the Service. Some of the Services are supported by advertising. Controls for how Microsoft personalizes advertising are available on the [Security & privacy page](#) of the Microsoft account management website. We do not use what you say in email, chat, video calls or voice mail, or your documents, photos or other personal files, to target advertising to you. Our advertising policies are covered in detail in the Privacy Statement.

[↑Top of page](#)

Group Messaging

Skype and GroupMe

Bing and MSN

Cortana

Outlook.com

Office-based Services

Microsoft Health
Services

Digital Goods

OneDrive

Microsoft Rewards

Azure

Binding Arbitration
and Class Action
Waiver

Miscellaneous

NOTICES

STANDARD
APPLICATION LICENSE
TERMS

Covered Services

Code of Conduct

3. Code of Conduct.

a. By agreeing to these Terms, you're agreeing that, when using the Services, you will follow these rules:

- i. Don't do anything illegal.
- ii. Don't engage in any activity that exploits, harms, or threatens to harm children.
- iii. Don't send spam. Spam is unwanted or unsolicited bulk email, postings, contact requests, SMS (text messages), or instant messages.
- iv. Don't publicly display or use the Services to share inappropriate content or material (involving, for example, nudity, bestiality, pornography, offensive language, graphic violence, or criminal activity).
- v. Don't engage in activity that is fraudulent, false or misleading (e.g., asking for money under false pretenses, impersonating someone else, manipulating the Services to increase play count, or affect rankings, ratings, or comments).
- vi. Don't circumvent any restrictions on access to or availability of the Services.
- vii. Don't engage in activity that is harmful to you, the Services or others (e.g., transmitting viruses, stalking, posting terrorist or violent extremist content, communicating hate speech, or advocating violence against others).
- viii. Don't infringe upon the rights of others (e.g., unauthorized sharing of copyrighted music or other copyrighted material, resale or other distribution of Bing maps, or photographs).
- ix. Don't engage in activity that violates the privacy of others.
- x. Don't help others break these rules.

b. **Enforcement.** If you violate these Terms, we may stop providing Services to you or we may close your Microsoft account. We may also block delivery of a communication (like email, file sharing or instant message) to or from the Services in an effort to enforce these Terms or we may remove or refuse to publish Your Content for any reason. When investigating alleged violations of these Terms, Microsoft reserves the right to review Your Content in order to resolve the issue. However, we cannot monitor the entire Services and make no attempt to do so.

c. **Application to Xbox Services.** Click [here](#) for more information about how this Code of Conduct applies to Xbox Live, Xbox Game Pass, Games for Windows Live and Xbox Game Studios games, applications, services and content provided by Microsoft. Violation of the Code of Conduct through Xbox Services (defined in section 14(a)(i)) may result in suspensions or bans from participation in Xbox Services, including forfeiture of content licenses, Xbox Gold Membership time, and Microsoft account balances associated with the account.

[↑Top of page](#)

Using the Services & Support

4. Using the Services & Support.

a. **Microsoft account.** You'll need a Microsoft account to access many of the Services. Your Microsoft account lets you sign in to products, websites and services provided by Microsoft and some Microsoft partners.

[↑Top of page](#)

Azure

n. **Azure.** Your use of the Azure service is governed by the terms and conditions of the separate agreement under which you obtained the services, as detailed at <https://go.microsoft.com/fwLink/?LinkId=522330>.

[↑Top of page](#)

Binding Arbitration and Class Action Waiver

15. **Binding Arbitration and Class Action Waiver If You Live In (or, If a Business, Your Principal Place of Business Is In) the United States.** We hope we never have a dispute, but if we do, you and we agree to try for 60 days to resolve it informally. If we can't, you and we agree to **binding individual arbitration before the American Arbitration Association ("AAA") under the Federal Arbitration Act ("FAA"), and not to sue in court in front of a judge or jury.** Instead, a neutral arbitrator will decide and the arbitrator's decision will be final except for a limited right of review under the FAA. **Class action lawsuits, class-wide arbitrations, private attorney-general actions, and any other proceeding where someone acts in a representative capacity aren't allowed. Nor is combining individual proceedings without the consent of all parties.** "We," "our," and "us" includes Microsoft, Skype (see section 10) and Microsoft's affiliates and, if you use Skype Pay by Mobile, your mobile phone carrier.

a. **Disputes Covered—Everything Except IP.** The term "dispute" is as broad as it can be. It includes any claim or controversy between you and us concerning the Services, the software related to the Services, the Services' or software's price, your Microsoft account, advertising, marketing, communications, your purchase transaction, billing, or these Terms, under any legal theory including contract, warranty, tort, statute, or regulation, **except disputes relating to the enforcement or validity of your, your licensors', our, or our licensors' intellectual property rights.**

b. **Mail a Notice of Dispute First.** If you have a dispute and our customer service representatives can't resolve it, send a Notice of Dispute by U.S. Mail to **Microsoft Corporation, ATTN: CELA Arbitration, One Microsoft Way, Redmond, WA 98052-6399, U.S.A.** (or to your mobile phone carrier at its principal place of business in the United States marked ATTN: Legal Department). Tell us your name, address, how to contact you, what the problem is, and what you want. A form is available at <https://go.microsoft.com/fwlink/?LinkId=245499>. We'll do the same if we have a dispute with you. After 60 days, you or we may start an arbitration if the dispute is unresolved.

c. **Small Claims Court Option.** Instead of mailing a Notice of Dispute, you may sue us in small claims court in your county of residence (or, if a business, your principal place of business) or King County, Washington, U.S.A. if you meet the court's requirements.

d. **Arbitration Procedure.** The AAA will conduct any arbitration under its Commercial Arbitration Rules (or if you are an individual and use the Services for personal or household use, or if the value of the dispute is \$75,000 or less whether or not you are an individual or how you use the Services, its Consumer Arbitration Rules). For more information, see www.adr.org or call 1-800-778-7879. To start an arbitration, submit the form available at

<https://go.microsoft.com/fwlink/?LinkId=245497> to the AAA and mail a copy to us. In a dispute involving \$25,000 or less, any hearing will be telephonic unless the arbitrator finds good cause to hold an in-person hearing instead. Any in-person hearing will take place in your county of residence (or, if a business, your principal place of business) or our principal place of business—King County, Washington if your dispute is with Microsoft. You choose. The arbitrator may award the same damages to you individually as a court could. The arbitrator may award declaratory or injunctive relief only to you individually to satisfy your individual claim. Under AAA Rules, the arbitrator rules on his or her own jurisdiction, including the arbitrability of any claim. But a court has exclusive authority to enforce the prohibition on arbitration on a class-wide basis or in a representative capacity.

e. Arbitration Fees and Payments.

i. **Disputes Involving \$75,000 or Less.** We will promptly reimburse your filing fees and pay the AAA's and arbitrator's fees and expenses. If you reject our last written settlement offer made before the arbitrator was appointed, your dispute goes all the way to an arbitrator's decision (called an "award"), and the arbitrator awards you more than this last written offer, we will: (i) pay the greater of the award or \$1,000; (ii) pay your reasonable attorney's fees, if any; and (iii) reimburse any expenses (including expert witness fees and costs) that your attorney reasonably accrues for investigating, preparing, and pursuing your claim in arbitration.

ii. **Disputes Involving More than \$75,000.** The AAA rules will govern payment of filing fees and the AAA's and arbitrator's fees and expenses.

f. **Conflict with AAA Rules.** These Terms govern to the extent they conflict with the AAA's Commercial Arbitration Rules or Consumer Arbitration Rules.

g. **Must File Within One Year.** You and we must file in small claims court or arbitration any claim or dispute (except intellectual property disputes—see section 15(a)) within one year from when it first could be filed. Otherwise, it's permanently barred.

h. **Rejecting Future Arbitration Changes.** You may reject any change we make to section 15 (except address changes) by sending us notice within 30 days of the change by U.S. Mail to the address in section 15(b). If you do, the most recent version of section 15 before the change you rejected will apply.

i. **Severability.** If any part of section 15 (Binding Arbitration and Class Action Waiver) is found to be illegal or unenforceable, the remainder will remain in effect (with an arbitration award issued before any court proceeding begins), except that if a finding of partial illegality or unenforceability would allow class-wide or representative arbitration, section 15 will be unenforceable in its entirety.

j. **Mobile Phone Carrier as Third-Party Beneficiary.** If you use Skype Pay by Mobile, your mobile phone carrier is a third-party beneficiary of your agreement with Microsoft and Skype to resolve disputes through informal negotiation and arbitration. Your mobile phone carrier agrees to do everything Microsoft and Skype agree to do in section 15.

[↑Top of page](#)

Miscellaneous

16. **Miscellaneous.** This section, and sections 1, 9 (for amounts incurred before the end of these Terms), 10, 11, 12, 13, 15, 18 and those that by their terms apply after the Terms end will survive any termination or cancellation of these Terms. We may assign these Terms, in whole or in part,

EXCERPTED EXHIBIT 2

6/25/2020

Microsoft Privacy Statement – Microsoft privacy

[Skip to main content](#)

Microsoft

Microsoft

[Privacy](#)[Privacy](#)[Privacy](#)

- [Home](#)
- [Our commitment to privacy](#)
- [Privacy dashboard](#)
- [Privacy report](#)
- [Privacy resources](#)
- [Privacy Statement](#)
- [More](#)

Microsoft Privacy Statement

Last Updated: May 2020 [What's new?](#)

[Collapse All](#)

[Print](#)

Your privacy is important to us. This privacy statement explains the personal data Microsoft processes, how Microsoft processes it, and for what purposes.

Microsoft offers a wide range of products, including server products used to help operate enterprises worldwide, devices you use in your home, software that students use at school, and services developers use to create and host what's next. References to Microsoft products in this statement include Microsoft services, websites, apps, software, servers, and devices.

Please read the product-specific details in this privacy statement, which provide additional relevant information. This statement applies to the interactions Microsoft has with you and the Microsoft products listed below, as well as other Microsoft products that display this statement.

[Personal data we collect](#)

[How we use personal data](#)

[Reasons we share personal data](#)

[How to access and control your personal data](#)

[Cookies and similar technologies](#)

[Products provided by your organization—notice to end users](#)

[Microsoft account](#)

[Other important privacy information](#)

[Security of personal data](#)

[Where we store and process personal data](#)

[Our retention of personal data](#)

[California Consumer Privacy Act](#)

[Advertising](#)

[Collection of data from children](#)

6/25/2020

Microsoft Privacy Statement – Microsoft privacy

event, we collect the data you provide to us when registering for or during the event and if you enter into a prize promotion, we collect the data you input into the entry form.

Content. Content of your files and communications you input, upload, receive, create, and control. For example, if you transmit a file using Skype to another Skype user, we need to collect the content of that file to display it to you and the other user. If you receive an email using Outlook.com, we need to collect the content of that email to deliver it to your inbox, display it to you, enable you to reply to it, and store it for you until you choose to delete it. Other content we collect when providing products to you include:

- Communications, including audio, video, text (typed, inked, dictated, or otherwise), in a message, email, call, meeting request, or chat.
- Photos, images, songs, movies, software, and other media or documents you store, retrieve, or otherwise process with our cloud.

Video or recordings. Recordings of events and activities at Microsoft buildings, retail spaces, and other locations. If you enter Microsoft Store locations or other facilities, or attend a Microsoft event that is recorded, we may process your image and voice data.

Feedback and ratings. Information you provide to us and the content of messages you send to us, such as feedback, survey data, and product reviews you write.

Product-specific sections below describe data collection practices applicable to use of those products.

[View Summary](#)

[Top of page](#)

How we use personal data

Microsoft uses the data we collect to provide you rich, interactive experiences. In particular, we use data to:

- Provide our products, which includes updating, securing, and troubleshooting, as well as providing support. It also includes sharing data, when it is required to provide the service or carry out the transactions you request.
- Improve and develop our products.
- Personalize our products and make recommendations.
- Advertise and market to you, which includes sending promotional communications, targeting advertising, and presenting you relevant offers.

We also use the data to operate our business, which includes analyzing our performance, meeting our legal obligations, developing our workforce, and doing research.

For these purposes, we combine data we collect from different contexts (for example, from your use of two Microsoft products). For example, Cortana may use information from your calendar to suggest action items in a heads-up email, and Microsoft Store uses information about the apps and services you use to make personalized app recommendations. However, we have built in technological and procedural safeguards designed to prevent certain data combinations where required by law. For example, where required by law, we store data we collect from you when you are unauthenticated (not

6/25/2020

Microsoft Privacy Statement – Microsoft privacy

activation.

- **Product development.** We use data to develop new products. For example, we use data, often de-identified, to better understand our customers' computing and productivity needs which can shape the development of new products.
- **Customer support.** We use data to troubleshoot and diagnose product problems, repair customers' devices, and provide other customer care and support services, including to help us provide, improve, and secure the quality of our products, services, and training, and to investigate security incidents. Call recording data may also be used to authenticate or identify you based on your voice to enable Microsoft to provide support services and investigate security incidents.
- **Help secure and troubleshoot.** We use data to help secure and troubleshoot our products. This includes using data to protect the security and safety of our products and customers, detecting malware and malicious activities, troubleshooting performance and compatibility issues to help customers get the most out of their experiences, and notifying customers of updates to our products. This may include using automated systems to detect security and safety issues.
- **Safety.** We use data to protect the safety of our products and our customers. Our security features and products can disrupt the operation of malicious software and notify users if malicious software is found on their devices. For example, some of our products, such as Outlook or OneDrive, systematically scan content in an automated manner to identify suspected spam, viruses, abusive actions, or URLs that have been flagged as fraud, phishing, or malware links; and we reserve the right to block delivery of a communication or remove content if it violates our terms.
- **Updates.** We use data we collect to develop product updates and security patches. For example, we may use information about your device's capabilities, such as available memory, to provide you a software update or security patch. Updates and patches are intended to maximize your experience with our products, help you protect the privacy and security of your data, provide new features, and ensure your device is ready to process such updates.
- **Promotional communications.** We use data we collect to deliver promotional communications. You can sign up for email subscriptions and choose whether you wish to receive promotional communications from Microsoft by email, SMS, physical mail, and telephone. For information about managing your contact data, email subscriptions, and promotional communications, see the [How to access and control your personal data](#) section of this privacy statement.
- **Relevant offers.** Microsoft uses data to provide you with relevant and valuable information regarding our products. We analyze data from a variety of sources to predict the information that will be most interesting and relevant to you and deliver such information to you in a variety of ways. For example, we may predict your interest in gaming and communicate with you about new games you may like.
- **Advertising.** Microsoft does not use what you say in email, chat, video calls, or voice mail, or your documents, photos, or other personal files to target ads to you. We use data we collect through our interactions with you, through some of our products, and on third-party web properties, for advertising in our products and on third-party properties. We may use automated processes to help make advertising more relevant to you. For more information about how your data is used for advertising, see the [Advertising](#) section of this privacy statement.
- **Prize promotions and events.** We use your data to administer prize promotions and events available in our physical Microsoft Stores. For example, if you enter into a prize promotion, we

6/25/2020

Microsoft Privacy Statement – Microsoft privacy

may use your data to select a winner and provide the prize to you if you win. Or, if you register for a coding workshop or gaming event, we will add your name to the list of expected attendees.

- **Transacting commerce.** We use data to carry out your transactions with us. For example, we process payment information to provide customers with product subscriptions and use contact information to deliver goods purchased from the Microsoft Store.
- **Reporting and business operations.** We use data to analyze our operations and perform business intelligence. This enables us to make informed decisions and report on the performance of our business.
- **Protecting rights and property.** We use data to detect and prevent fraud, resolve disputes, enforce agreements, and protect our property. For example, we use data to confirm the validity of software licenses to reduce piracy. We may use automated processes to detect and prevent activities that violate our rights and the rights of others, such as fraud.
- **Legal compliance.** We process data to comply with law. For example, we use the age of our customers to ensure we meet our obligations to protect children's privacy. We also process contact information and credentials to help customers exercise their data protection rights.
- **Research.** With appropriate technical and organizational measures to safeguard individuals' rights and freedoms, we use data to conduct research, including for public interest and scientific purposes.

[View Summary](#)

[Top of page](#)

Reasons we share personal data

We share your personal data with your consent or as necessary to complete any transaction or provide any product you have requested or authorized. For example, we share your content with third parties when you tell us to do so, such as when you send an email to a friend, share photos and documents on OneDrive, or link accounts with another service. If you use a Microsoft product provided by an organization you are affiliated with, such as an employer or school, or use an email address provided by such organization to access Microsoft products, we share certain data, such as interaction data and diagnostic data to enable your organization to manage the products. When you provide payment data to make a purchase, we will share payment data with banks and other entities that process payment transactions or provide other financial services, and for fraud prevention and credit risk reduction.

In addition, we share personal data among Microsoft-controlled affiliates and subsidiaries. We also share personal data with vendors or agents working on our behalf for the purposes described in this statement. For example, companies we've hired to provide customer service support or assist in protecting and securing our systems and services may need access to personal data to provide those functions. In such cases, these companies must abide by our data privacy and security requirements and are not allowed to use personal data they receive from us for any other purpose. We may also disclose personal data as part of a corporate transaction such as a merger or sale of assets.

Finally, we will retain, access, transfer, disclose, and preserve personal data, including your content (such as the content of your emails in Outlook.com, or files in private folders on OneDrive), when we have a good faith belief that doing so is necessary to do any of the following:

- Comply with applicable law or respond to valid legal process, including from law enforcement or other government agencies.

6/25/2020

Microsoft Privacy Statement – Microsoft privacy

- Protect our customers, for example, to prevent spam or attempts to defraud users of our products, or to help prevent the loss of life or serious injury of anyone.
- Operate and maintain the security of our products, including to prevent or stop an attack on our computer systems or networks.
- Protect the rights or property of Microsoft, including enforcing the terms governing the use of the services—however, if we receive information indicating that someone is using our services to traffic in stolen intellectual or physical property of Microsoft, we will not inspect a customer's private content ourselves, but we may refer the matter to law enforcement.

For more information about data we disclose in response to requests from law enforcement and other government agencies, please see our [Law Enforcement Requests Report](#).

Please note that some of our products include links to or otherwise enable you to access products of third parties whose privacy practices differ from those of Microsoft. If you provide personal data to any of those products, your data is governed by their privacy policies.

View Summary

[Top of page](#)

How to access and control your personal data

You can also make choices about the collection and use of your data by Microsoft. You can control your personal data that Microsoft has obtained, and exercise your data protection rights, by contacting Microsoft or using various tools we provide. In some cases, your ability to access or control your personal data will be limited, as required or permitted by applicable law. How you can access or control your personal data will also depend on which products you use. For example, you can:

- Control the use of your data for interest-based advertising from Microsoft by visiting our [opt-out page](#).
- Choose whether you wish to receive promotional emails, SMS messages, telephone calls, and postal mail from Microsoft.
- Access and clear some of your data through the [Microsoft privacy dashboard](#).

Not all personal data processed by Microsoft can be accessed or controlled via the tools above. If you want to access or control personal data processed by Microsoft that is not available via the tools above or directly through the Microsoft products you use, you can always contact Microsoft at the address in the [How to contact us](#) section or by using our [web form](#).

We provide aggregate metrics about user requests to exercise their data protection rights via the [Microsoft Privacy Report](#).

You can access and control your personal data that Microsoft has obtained with tools Microsoft provides to you, which are described below, or by contacting Microsoft. For instance:

- If Microsoft obtained your consent to use your personal data, you can withdraw that consent at any time.
- You can request access to, erasure of, and updates to your personal data.
- If you'd like to port your data elsewhere, you can use tools Microsoft provides to do so, or if none are available, you can contact Microsoft for assistance.

EXCERPTED EXHIBIT 3

**Microsoft Software, Devices, and Services with Arbitration Agreements
Consumer Demand for Arbitration before the
American Arbitration Association**

Instructions for filing an arbitration claim with American Arbitration Association:

1. Please fill out this form and keep a copy for your records.
2. **Mail a copy of this form and your check or money order for \$200 to American Arbitration Association, Case Filing Services, 1101 Laurel Oak Road, Suite 100, Voorhees, NJ 08043. Make your check or money order payable to American Arbitration Association. Please consult the AAA Consumer Arbitration Rules for more information. You can find them at www.adr.org or by calling the AAA at (800) 778-7879.**
3. **Please copy (or download and print) and mail to AAA (with this form and your check) your agreement with an arbitration clause (for example, Microsoft Services Agreement (for Xbox Live and most Microsoft services), Manufacturer's Limited Hardware Warranty & Agreement (for Xbox, Surface, mice, keyboards, cameras, and most Microsoft hardware), Microsoft Software License Terms Windows Operating System, etc.). If you don't have your agreement, you can find most at www.microsoft.com/en-us/Legal/arbitration/default.aspx**
4. **Mail a copy of this form, a copy of your Microsoft agreement, and a copy of your check or money order to Microsoft Corporation, CELA Arbitration, One Microsoft Way, Redmond, WA 98052-6399. Upon receipt, Microsoft will reimburse you for your \$200 filing fee if your claim is for \$75,000 or less.**

Your Information:

Name: Thomas Deutsch, Esq.

Address: 27 Scheurman Terrace

City/State/Zip: Warren, NJ 07059-7154

Phone: (917) 406-5648

Fax: _____

E-mail address: tomdeutsch@aol.com

tomdeutsch@aol.com

Gamertag (for Xbox)

Microsoft account (was Windows Live ID)

Disputes involving \$25,000 or less are usually resolved by the submission of documents. If a hearing is held, it will usually be telephonic. In disputes involving more than \$25,000, a telephonic or in-person hearing will be held. If in person, you may choose your home county or King County (Seattle area), Washington. Please tell us the county and state where you live:

Somerset
County

New Jersey
State

(please complete page two)

Your Attorney's Information (Please leave blank if you are representing yourself):

Attorney's Name: _____

Firm: _____

Address: _____

City/State/Zip: _____

Phone: _____ Fax: _____

E-mail address: _____

Briefly explain the nature of your dispute. You may use additional pages.

PLEASE SEE ATTACHED ADDENDUM

**TIME IS OF THE ESSENCE IN RESTORING MY ACCESS TO MY
DOCUMENTS TO RESOLVE THIS MATTER!!!**

How much money do you believe you are owed? If none, leave blank:

Over \$75,000 if my documents are not returned. Damages TBD depending on the timing of the return
\$ _____ of the documents.

Do you desire any non-monetary relief? If so, Yes X No _____

X what non-monetary relief?

PLEASE SEE ATTACHED ADDENDUM

Tom Deutsch
Signature

August 14, 2020
Date

**TIME IS OF THE ESSENCE IN RESTORING MY ACCESS TO MY
DOCUMENTS TO RESOLVE THIS MATTER!!!**

Statement of Facts

On or around October 17, 2019, I purchased Microsoft OneDrive, Microsoft 365 Personal (Order Number—MT0W0KTHTT) from iPhone from Seller Microsoft. In the ensuing months, I have been charged \$6.99 plus taxes for this service from Microsoft.

I signed up for this service relying on Microsoft's advertisement that my files AND their organization for "Any file, anywhere, always protected" (see Attachment A, which is the Microsoft landing/advertising page for OneDrive). Microsoft also advertises that they "Back up and protect. If you lose your device, you won't lose your files and photos when they're saved in OneDrive." Also, while using OneDrive, Microsoft continually refers to my documents being "Always" backed up once they are uploaded to OneDrive. Prior to transferring my files to OneDrive in October, 2019, I had my files stored on my home desktop hard drive.

Thereafter, I spent a great deal of time reorganizing my files solely on OneDrive as well as continued to add and modify documents, given the representations made in Microsoft advertising for OneDrive. I had a strong and reasonable belief that my files were safe from loss, which is precisely what Microsoft's intent is in their OneDrive advertising.

Sometime in April, 2020, I began to get a message on my computer that I needed to re-log into OneDrive. I attempted to do so multiple times over the span of a month, but it sent me to an error screen. At no point was I directly notified that my account had been suspended nor was I notified that my documents were not backing up to OneDrive.

I contacted Microsoft three times in writing through their system, but heard nothing back for over a month. Finally, I received the curt Attachment B email on May 27, 2019 (the "May 27 Email") informing me that my account access had been disabled "due to a serious violation of the Microsoft Services Agreement" (the "Services Agreement"). This was the first time I was exposed to the Services Agreement, as I had signed up for the service through iPhone, and had never seen or agreed to the Services Agreement. To date, I have not been provided any explanation or understanding of the nature of the 'serious violation' nor I have ever been accorded any opportunity to dispute that unilateral assertion.

The May 27 Email also relayed that “Microsoft will immediately cease charging the credit card on file for recurring charges.” In direct contravention to the Microsoft Services Agreement and the May 27 Email, my credit card was charged the usual \$6.99 charge on both June 21, 2020 as well as July 21, 2020 (see Attachments C & D).

On June 1, 2020, I immediately completed the Attachment D2 Notice of Dispute and mailed a hard copy to Microsoft’s specified address AND replied to the May 27 Email with a copy of the Notice of Dispute. To date, I have not received any response directly from the Microsoft “CELA Arbitration” unit.

I did receive the Attachment E email on June 5, 2020 (the “June 5 Email”) from a Customer Service Agent also reiterating the assertion that I had committed a “serious violation” of the Services Agreement, but then went further to say that my account “was properly closed” (rather than the May 27 Email saying my account had been ‘disabled’). The June 5 Email also states that “Pursuant to our terms, we cannot reactivate your account, nor provide details as to why it was closed.” The June 5 Email goes further to say that “This represents Microsoft’s final communication regarding this account.” Microsoft’s Services Agreement nevertheless specifies that I should have to wait 55 more days before I could avail myself of arbitration, which does not represent the same substantive rights as a small claims court action to seek immediate redress.

Shortly after the June 5 Email in mid-June, my desktop computer generated the attached Attachment F, which is colloquially termed the “Blue Screen of Death.” It is unclear to me what caused the Blue Screen of Death, but its effect on my computer, files and programs was extremely damaging. Both an IT professional and myself spent dozens of hours attempting to reinstall Microsoft Windows correctly, but when it was reinstalled, all of my files AND programs had been deleted from my hard drive. My IT professional installed and ran the Stellar Data Recovery program in attempt to recover my files, but all of the files the program recovered were ‘corrupted’ when I attempted to open them.

On June 24, I received the Attachment G email from Microsoft that specified that my “support case has been closed.”

As a consequence of these events, I currently only have my personal files as of October, 2019 and no updates to them or additional saved documents from then on. That loss represents hundreds, if not thousands, of hours of my personal time

creating and revising and organizing all of my computer records from my entire life.

Brief Analysis

1. I never saw or agreed to the Microsoft Services Agreement, since I signed up for the service through Apple/iPhone. The burden of proof is on Microsoft to demonstrate that the Services Agreement was available at the time of the consummation of the contract. Microsoft's continued charging of my credit card through their agent (Apple/iPhone) is prima facie evidence that their advertising and information dissemination is not seamless.
2. I wasn't notified of a breach of the Services Agreement until well over a month after the alleged breach occurred AND only after I had repeatedly followed up with Microsoft questioning why I wasn't able to access my documents. Microsoft under their own Services Agreement has an obligation to inform a user directly and explicitly if Microsoft asserts there has been a breach of contract that would rise to the level of termination. Had Microsoft informed me contemporaneously and directly of their suspension of service, I would have been able to mitigate damages from what I now allege is their breach of contract. Instead, I was left assuming that my documents were still being backed up and that this situation was just some kind of technical glitch.
3. Even if I had agreed to the Services Agreement, I would have never understood and agreed it to mean that Microsoft could cut off my service unilaterally and completely prevent me from ever again accessing any and all my computer files. The logical practical effect of that outcome would be any user would need to back up their documents to another device at every moment that user updated documents on OneDrive if that user wanted to ensure they wouldn't lose access to his newest work. Microsoft clearly advertises OneDrive as "Always" backing up documents and having them available to users "anytime" and on "any device." No asterisks or disclaimers are ever used on what would amount to false advertising if Microsoft could indeed prevent users from accessing their own documents. No user would ever reasonably expect that by signing up for Microsoft's OneDrive that the biggest risk to that user losing the man hours creating, revising and organizing their files is Microsoft's unilateral decision making to intentionally deprive that user of his access to his own files.
4. Microsoft can not unilaterally declare a "serious violation" under the Services Agreement that is not subject to review by either its counterparty or through small claims court or arbitration. A Microsoft Customer Support

agent's view of a material violation of the Agreement and a counterparty or court's view of materiality may be very different. Under that standard, Microsoft could terminate service to all its users and not be subject to any contractual damages or recourse from counterparties whatsoever. That is a plainly absurd and unconscionable legal view that contradicts centuries of contract and common law as well as any concept of legal equity. To further articulate this absurdity with an example, if I had the formula for the vaccine for COVID-19 on my OneDrive account, Microsoft asserts that they can block me, and without any prior notice, from accessing that important and valuable document because Microsoft believes in their sole and indisputable opinion that I have something in my files that violates their terms of service.

5. Microsoft owes me a duty to disclose whatever my alleged violation is. It appears clear that Microsoft wants to conceal what or how they find out users are breaching the Services Agreement. Although the perceived 'spying' by Microsoft onto their users content may be the driving force for Microsoft's internal policy, Microsoft may not ignore their obligation to subject their assertions to counterparty and/or court review.
6. Even if Microsoft could unilaterally terminate the contract, Microsoft specifically did NOT terminate the contract, but instead explicitly chose to continue the contract. Microsoft continued to charge my credit card through its intermediary (Apple/iPhone), in direct contravention of both its representative's written May 17 Email as well as the Microsoft Services Agreement. Yet, since April, 2020 through the date of this submission, I have no had any access to OneDrive or the other services that I have continued to pay for and thereby have contractual rights to. If Microsoft wants to assert some sort of absurd punctilious adherence to its Services Agreement, then they must subject themselves to said punctiliousness. As a legal matter, Microsoft was clearly the author of the Services Agreement, so any and all ambiguities must be interpreted against them.
7. Even if all of the above would be dismissed, Microsoft would still be liable for return of my documents for the damages caused by its Blue Screen of Death. No user should lose all of their documents off of their hard drive due to some deficiency in the Windows operating system. Moreover, no user should lose all their documents when the precise instance where they are separately paying Microsoft to "Always" have those documents backed up and available to the user on all of his "Devices." That practical piece of mind is precisely Microsoft's advertising campaign for OneDrive and

precisely why users like myself paid extra for that document retention and protection.

What non-monetary relief

1. A detailed description from Microsoft of what the “serious violation” of the Microsoft Services Agreement. I would not have knowingly and intentionally violate the Services Agreement. As I have signed up for an alternate services provider, it is imperative I know whatever violation is alleged, so I don’t run afoul of any other provider’s services agreement.
2. Return of all my documents stored on OneDrive as of the most recent date that I saved the latest onto OneDrive.
3. A complimentary copy of the latest version of Microsoft Office Home & Business for all of my personal devices to replace my version lost to the ‘Blue Screen of Death’ and the time lost on this process.

I’m am primarily looking to get access to my own documents in the organization that I had them in, but the longer my access to my documents and organization is prevented, the higher the pecuniary damages will be.

**TIME IS OF THE ESSENCE IN RESTORIONG MY ACCESS TO MY
DOCUMENTS TO RESOLVE THIS MATTER!!!**

8/13/2020

Your receipt from Apple.

Subject: **Your receipt from Apple.**
 Date: 6/21/2020 9:17:24 PM Eastern Standard Time
 From: no_reply@email.apple.com
 To: tomdeutsch@aol.com

Attachment

Receipt

Save 3% on all your Apple purchases with Apple Card. Apply and use in minutes

APPLE ID
tomdeutsch@aol.com

DATE
Jun 21, 2020

ORDER ID
MT0YL1B45S

DOCUMENT NO.
172351686831

BILLED TO
Visa 4259
Thomas Deutsch
27 Scheurman Terrace
Warren, NJ 07059-7154
USA

App Store



Microsoft 365 Personal (Automatic Renewal)
 Microsoft 365 Personal (Automatic Renewal) (Monthly)
 Renews Jul 17, 2020

\$6.99

[Write a Review](#) | [Report a Problem](#)

Subtotal **\$6.99**
 Tax **\$0.46**

TOTAL \$7.45



Save 3% on all your Apple purchases.



Apply and use in minutes

Privacy: We use a Subscriber ID to provide reports to developers.
 Get help with subscriptions and purchases. Visit Apple Support. Learn how to manage your password preferences for
 iTunes, Apple Books, and App Store purchases.

EXCERPTED EXHIBIT 4

CONSUMER

Consumer Arbitration Rules



AMERICAN ARBITRATION ASSOCIATION®

Available online at adr.org/consumer

Rules Amended and Effective September 1, 2014

Cost of Arbitration Effective January 1, 2016

The American Arbitration Association, founded in 1926, is a neutral, independent, and private not-for-profit organization. We offer a broad range of conflict management services to businesses, organizations, and individuals. We also provide education, training, and publications focused on methods for settling disputes out of court.

The Arbitrator

Except where the parties to a case reach their own settlement, the arbitrator will make the final, binding decision called the Award on the dispute and render it in writing. The Arbitrator makes all the procedural decisions on a case not made by the Administrator or not decided jointly by the parties. The arbitrator may grant any remedy, relief, or outcome that the parties could have received in court, including awards of attorney's fees and costs, in accordance with the law or laws that apply to the case.

Arbitrators are neutral and independent decision makers who are not employees of the AAA. Once appointed to a case, an arbitrator may not be removed by one party without the other party's consent or unless the Administrator determines an arbitrator should be removed and replaced by another arbitrator chosen by the Administrator in a manner described in these Rules.

The AAA's Consumer Arbitration Rules

The AAA has developed the *Consumer Arbitration Rules* for consumers and businesses that want to have their disagreements resolved through arbitration.

Availability of Mediation through [Mediation.org](https://www.mediation.org)

Mediation in consumer disputes is also available to help parties resolve their disputes. Parties interested in participating in mediation may find a mediator through **www.mediation.org**.

Administrative Fees

The Association charges a fee for its services under these Rules. A fee schedule is included at the end of these Rules in the Costs of Arbitration section.

Pre-Hearing Preparation

R-21. Preliminary Management Hearing with the Arbitrator

- (a) If any party asks for, or if the AAA or the arbitrator decides to hold one, the arbitrator will schedule a preliminary management hearing with the parties and/or their representatives as soon as possible. The preliminary management hearing will be conducted by telephone unless the arbitrator decides an in-person preliminary management hearing is necessary.
- (b) During the preliminary management hearing, the parties and the arbitrator should discuss the future conduct of the case, including clarification of issues and claims, scheduling of the hearings, and any other preliminary matters.
- (c) The arbitrator shall promptly issue written orders that state the arbitrator's decisions made during or as a result of the preliminary management hearing. The arbitrator may also conduct additional preliminary management hearings if the need arises.

R-22. Exchange of Information between the Parties

- (a) If any party asks or if the arbitrator decides on his or her own, keeping in mind that arbitration must remain a fast and economical process, the arbitrator may direct
 - 1) specific documents and other information to be shared between the consumer and business, and
 - 2) that the consumer and business identify the witnesses, if any, they plan to have testify at the hearing.
- (b) Any exhibits the parties plan to submit at the hearing need to be shared between the parties at least five business days before the hearing, unless the arbitrator sets a different exchange date.
- (c) No other exchange of information beyond what is provided for in section (a) above is contemplated under these Rules, unless an arbitrator determines further information exchange is needed to provide for a fundamentally fair process.
- (d) The arbitrator has authority to resolve any disputes between the parties about exchanging information.

R-23. Enforcement Powers of the Arbitrator

The arbitrator may issue any orders necessary to enforce the provisions of rules R-21 and R-22 and to otherwise achieve a fair, efficient, and economical resolution of the case, including, but not limited to:

- (a) an order setting the conditions for any exchange or production of confidential documents and information, and the admission of confidential evidence at the hearing in order to preserve such confidentiality;

- (b) to the extent the exchange of information takes place pursuant to R-22, imposing reasonable search limitations for electronic and other documents if the parties are unable to agree;
- (c) allocating costs of producing documentation, including electronically-stored documentation;
- (d) in the case of willful non-compliance with any order issued by the arbitrator, drawing adverse inferences, excluding evidence and other submissions, and/or making special allocations of costs or an interim award of costs arising from such non-compliance; and
- (e) issuing any other enforcement orders that the arbitrator is empowered to issue under applicable law.

R-24. Written Motions (except for Dispositive Motions—see R-33)

The arbitrator may consider a party's request to file a written motion (except for Dispositive Motions— see R-33) only after the parties and the arbitrator conduct a conference call to attempt to resolve the issue that gives rise to the proposed motion. Only after the parties and the arbitrator hold the call may the arbitrator consider a party's request to file a written motion. The arbitrator has the sole discretion to allow or deny the filing of a written motion and his or her decision is final.

R-25. Representation of a Party

Any party may participate in the arbitration without representation, or may be represented by counsel or other authorized representative, unless such choice is prohibited by applicable law. A party intending to be represented shall give the opposing party and the AAA the name, address, and contact information of the representative at least three business days before the hearing where that representative will first appear in the case. It will be considered proper notice if a representative files the arbitration demand or answer or responds for a party during the course of the arbitration.

While parties do not need an attorney to participate in arbitration, arbitration is a final, legally-binding process that may impact a party's rights. As such, parties may want to consider consulting an attorney.

R-33. Dispositive Motions

The arbitrator may allow the filing of a dispositive motion if the arbitrator determines that the moving party has shown substantial cause that the motion is likely to succeed and dispose of or narrow the issues in the case.

R-34. Evidence

- (a) The parties may offer relevant and material evidence and must produce any evidence the arbitrator decides is necessary to understand and decide the dispute. Following the legal rules of evidence shall not be necessary. All evidence should be taken in the presence of the arbitrator and all of the parties, unless any of the parties is absent, in default, or has waived the right to be present.
- (b) The arbitrator shall determine what evidence will be admitted, what evidence is relevant, and what evidence is material to the case. The arbitrator may also exclude evidence that the arbitrator decides is cumulative or not relevant.
- (c) The arbitrator shall consider applicable principles of legal privilege, such as those that involve the confidentiality of communications between a lawyer and a client.
- (d) An arbitrator or other person authorized by law to subpoena witnesses or documents may do so on the request of any party or on the arbitrator's own determination. If a party requests the arbitrator sign a subpoena, that party shall copy the request to the other parties in the arbitration at the same time it is provided to the arbitrator.

R-35. Evidence by Affidavit and Post-Hearing Filing of Documents or Other Evidence

- (a) The arbitrator may receive and consider the evidence of witnesses by declaration or affidavit rather than in-person testimony but will give this evidence only such credence as the arbitrator decides is appropriate. The arbitrator will consider any objection to such evidence made by the opposing party.
- (b) If the parties agree or the arbitrator decides that documents or other evidence need to be submitted to the arbitrator after the hearing, those documents or other evidence will be filed with the AAA so that they can be sent to the arbitrator. All parties will be given the opportunity to review and respond to these documents or other evidence.

R-36. Inspection or Investigation

An arbitrator finding it necessary to inspect property or conduct an investigation in connection with the arbitration will request that the AAA inform the parties. The arbitrator will set the date and time of the inspection and investigation, and

EXHIBIT 5



AMERICAN
ARBITRATION
ASSOCIATION®

INTERNATIONAL CENTRE
FOR DISPUTE RESOLUTION®

Northeast Case Management Center
1301 Atwood Avenue
Suite 211N
Johnston, RI 02919
Telephone: (866)293-4053
Fax: (866)644-0234

November 9, 2020

Thomas Deutsch, Esq.
27 Scheurman Terrace
Warren, NJ 07059-7154
Via Email to: tomdeutsch@aol.com

Natalie Nahabet, Esq.
Orrick, Herrington & Sutcliffe
777 South Figueroa Street, Suite 3200
Los Angeles, CA 90017
Via Email to: nnahabet@orrick.com

Case Number: 01-20-0014-3715

Thomas Deutsch, Esq.
-vs-
Microsoft Corporation

Dear Parties:

Per the applicable Consumer Arbitration Rules, the American Arbitration Association (AAA) has made an administrative appointment of Hon. Harriet Derman, J.S.C. (ret) to serve as arbitrator. Enclosed please find the Notice of Appointment and General Arbitrator Oath Form, the Notice of Compensation Arrangements for consumer cases as well as the arbitrator's resume.

Please advise the AAA of any factual objections to the appointment of the arbitrator within five (5) business days of the date of this letter, by **November 16, 2020**. Copies of the objection are to be provided to all parties. However, the arbitrator shall not be copied on any correspondence regarding objections to their service.

If any objections are received, the other party will be given an opportunity to respond before the AAA makes a determination, in accordance with the Rules, regarding the arbitrator's continued service.

As requested by the arbitrator, and specified in the Consumer Arbitration Rules, the parties and their representatives must provide information to the AAA of any circumstances likely to raise justifiable doubt as to whether the arbitrator can remain impartial or independent. Further, such obligation to provide disclosure information remains in effect throughout the arbitration.

As a final point, we remind you of Consumer Rule R-9. This rule states "after the arbitrator is appointed, if a party wants to take the case to small claims court and notifies the opposing party and the AAA, it is up to the arbitrator to determine if the case should be decided in arbitration or if the arbitration case should be closed and the dispute decided in small claims court."

Sincerely,

/s/

Jenna Pascale

Case Administrator

Direct Dial: (401)406-7095

Email: jennapascale@adr.org

Supervisor Information: *Jennifer Rego; RegoJ@adr.org*

Enclosures

bcc:

Hon. Harriet Derman, J.S.C. (ret)

cc:

Marc Shapiro

Yana Rosenbloom

General Arbitrator Oath Form

American Arbitration Association

Thomas Deutsch, Esq.

Vs.

Microsoft Corporation

Case# 01-20-0014-3715

Notice of Appointment for Hon. Harriet Derman, J.S.C. (ret)

Disclosure Obligations

It is most important that the parties have complete confidence in the arbitrator's impartiality. Therefore, please disclose any past or present relationship with the parties, their counsel, or potential witnesses, direct or indirect, whether financial, professional, social or of any other kind. This is a continuing obligation throughout your service on the case and should any additional direct or indirect contact arise during the course of the arbitration or if there is any change at any time in the biographical information that you have provided, it must also be disclosed. Any doubts should be resolved in favor of disclosure. If you are aware of direct or indirect contact with such individuals, please describe it below. Failure to make timely disclosures may forfeit your ability to collect compensation. All disclosures will be brought to the attention of the parties.

Instructions

You will not be able to serve until this duly executed Notice of Appointment has been completed and submitted. Please review the *Disclosure Guidelines* found by navigating to the *My Tasks* screen from the menu on the left, and after conducting a conflicts check, answer the following questions and complete the remainder of this Notice of Appointment.

Should the answer to any of the following questions be "Yes", or if you are aware of any other information that may lead to a justifiable doubt as to your impartiality or independence or create an appearance of partiality, then describe the nature of the potential conflict(s) in the space provided.

1. Do you or your law firm presently represent any person in a proceeding involving any party to the arbitration?

Answer : NO

2. Have you represented any person against any party to the arbitration?

Answer : NO

3. Have you had any professional or social relationship with counsel for any party in this proceeding or the firms for which they work?

Answer : NO

4. Have you had any professional or social relationship with any parties or witnesses identified to date in this proceeding or the entities for which they work?

Answer : NO

5. Have you had any professional or social relationship of which you are aware with any relative of any of the

General Arbitrator Oath Form

parties to this proceeding, or any relative of counsel to this proceeding, or any of the witnesses identified to date in the proceeding?

Answer : NO

6. Have you, any member of your family, or any close social or business associate ever served as a neutral in a proceeding in which any of the identified witnesses or named individual parties gave testimony?

Answer : NO

7. Have you, any member of your family, or any close social or business associate been involved in the last five years in a dispute involving the subject matter contained in the case which you are assigned?

Answer : NO

8. Have you ever served as an expert witness or consultant to any party, attorney, witness or other arbitrator identified in this case?

Answer : NO

9. Have any of the party representatives, law firms or parties appeared before you in past arbitration cases?

Answer : NO

10. Are you a member of any organization that is not listed on your panel biography that may be relevant to this arbitration?

Answer : NO

11. Have you ever sued or been sued by either party or its representative?

Answer : NO

12. Do you or your spouse own stock in any of the companies involved in this arbitration?

Answer : YES

Comments : I have at least \$70,000 worth of Microsoft stock in a managed brokerage account. In other words, I did not purchase or even know if I owned Microsoft stock, but I checked my brokerage statement and found the amount as set forth. I still believe I could be fair and impartial.

13. If there is more than one arbitrator appointed to this case, have you had any professional or social relationships with any of the other arbitrators?

Answer : NO

14. Are there any connections, direct or indirect, with any of the case participants that have not been covered by the above questions?

Answer : NO

15. Are you aware of any other information that may lead to a justifiable doubt as to your impartiality or

General Arbitrator Oath Form

independence or create an appearance of partiality?

Answer : NO

Arbitrator's Oath

I attest that I have reviewed my biographical information provided to the parties on this case and confirm it is current, accurate and complete.

I attest that I have diligently conducted a conflicts check, including a thorough review of the information provided to me about this case to date, and that I have performed my obligations and duties to disclose in accordance with the Rules of the American Arbitration Association, Code of Ethics for Arbitrators in Commercial Disputes, the parties' agreement, and applicable law pertaining to arbitrator disclosures.

I further affirm that consistent with the applicable Rules of the American Arbitration Association, the Code of Ethics for Arbitrators in Commercial Disputes, the parties' agreement, and applicable law:

- That I am fit to serve on the above-referenced arbitration and able to fully execute my responsibilities during all phases of the case;
- That I will keep confidential all matters relating to the above-referenced arbitration;
- That I will maintain a professional demeanor and appearance of impartiality during all phases of this case;
- That I will endeavor to effectively manage all phases of this case with a commitment to speed, economy and just resolution in a manner consistent with the parties' expectations;
- That I will bill parties responsibly and ethically and will review my bills for reasonableness relative to the nature and scope of the activity performed prior to submitting them to the AAA.

The arbitrator being duly sworn, hereby accepts this appointment.

Terms of Compensation

Before proceeding, please indicate that you have reviewed the Notice of Compensation Arrangements for this case.



Once completed, please indicate your acceptance of this appointment as arbitrator by entering your initials in the space provided.

(hed)

Hon. Harriet Derman, J.S.C. (ret)
3-Nov-20

EXHIBIT 6



AMERICAN
ARBITRATION
ASSOCIATION®

INTERNATIONAL CENTRE
FOR DISPUTE RESOLUTION®

Northeast Case Management Center
1301 Atwood Avenue
Suite 211N
Johnston, RI 02919
Telephone: (866)293-4053
Fax: (866)644-0234

November 20, 2020

Thomas Deutsch, Esq.
27 Scheurman Terrace
Warren, NJ 07059-7154
Via Email to: tomdeutsch@aol.com

Natalie Nahabet, Esq.
Orrick, Herrington & Sutcliffe
777 South Figueroa Street, Suite 3200
Los Angeles, CA 90017
Via Email to: nnahabet@orrick.com

Case Number: **01-20-0014-3715**
Thomas Deutsch, Esq.
-vs-
Microsoft Corporation

Dear Parties:

This will confirm the appointment of Hon. Harriet Derman, J.S.C. (ret) as arbitrator in this matter.

As requested by the arbitrator, if either party or their counsel knows of any contact or conflict that may be relevant, they are to communicate this information to the American Arbitration Association (AAA) immediately.

This will acknowledge receipt of the payment of the Case Management Fee; therefore, we will proceed with scheduling a telephonic Preliminary Hearing.

In order to schedule this hearing, please utilize the online calendar at the following link:

<https://www.when2meet.com/?10391948-Jy31i>

Instructions for utilizing the online calendar:

- Click on the link.
- Type in your full name next to “sign in.”
- Type in any password you want (there is no need to set up a profile or account).
- Highlight the times you are available.
- Everyone’s availability will show on the calendar as they enter it and will reveal mutual times to schedule the call.
- When done, simply close the web page (there is no need to save; to confirm your updates registered, simply click back on the original link).

All times displayed on the online calendar reflect your local time zone.

Please provide your availability on or before November 24, 2020. If we do not receive a response, we will

presume all options are acceptable and a telephonic preliminary hearing will be set.

Sincerely,

/s/

Jenna Pascale

Case Administrator

Direct Dial: (401)406-7095

Email: jennapascale@adr.org

Supervisor Information: *Jennifer Rego*, RegoJ@adr.org

bcc:

Hon. Harriet Derman, J.S.C. (ret)

cc:

Marc Shapiro

Yana Rosenbloom

EXHIBIT 7

From: Harriet Derman <hderman@newjerseylaw.net>
Sent: Thursday, December 3, 2020 11:07 AM
To: AAA Jenna Pascale; tomdeutsch@aol.com; Nahabet, Natalie
Subject: Order of Arbitrator in Deutsch v. Microsoft Corp.

A hearing was held on December 3, 2020. Mr. Deutsch was self-represented. Respondent was represented by Ms. Nahabet and Mr. Shapiro. In lieu of completing the Report of Preliminary Management Hearing and Scheduling Order at this time ("Report and Scheduling Order"), it was agreed as follows:

1. Claimant shall file his amended claim no later than December 10, 2020.
2. Respondent shall file its response to the amended claim no later than December 23, 2020.
3. Claimant shall file his application for emergent relief no later than December 10, 2020.
4. Respondent shall file its opposition no later than December 31, 2020.
5. Claimant shall file his reply no later than January 6, 2021.
6. Oral argument shall be conducted on January 14 at 3:00 pm (Eastern).
7. Completion of the Report and Scheduling Order would take place immediately following the oral argument referenced in #6. This Report and Scheduling Order will provide a schedule for Respondent to file a dispositive motion.
8. All documents shall be direct exchange and not through AAA.
9. All documents exceeding 10 pages should be sent to the addresses provided by the Arbitrator as follows:

Up to and including December 31: 34 Rayle Court, Metuchen, NJ 08840, NO SIGNATURE REQUIRED.

After December 31: c/o Olsen, 521 Putting Green, Longboat Key, FL, 34228. NO SIGNATURE REQUIRED.

Harriet Derman,

Arbitrator

EXCERPTED EXHIBIT 8

AMERICAN ARBITRATION ASSOCIATION

THOMAS DEUTSCH, ESQ.,	:	
	:	
<i>Claimant,</i>	:	CASE NO. 01-20-0014-3715
	:	
v.	:	
	:	
MICROSOFT CORPORATION,	:	
	:	
<i>Respondent.</i>	:	

RESPONDENT MICROSOFT CORPORATION’S
OPPOSITION TO CLAIMANT’S MOTION SEEKING EMERGENT RELIEF

Microsoft does not search its customers' private files, and PhotoDNA does not run against private files. *Id.* It is only when a customer shares an image from his or her OneDrive account, or makes an image from his or her OneDrive account public—e.g., puts the image in a non-private state—that PhotoDNA is triggered. *Id.*

Once an image is confirmed to be CSEAI, Microsoft suspends the account under the MSA to prevent further dissemination of CSEAI. *Id.* ¶ 11. In addition, Microsoft sends a report to NCMEC, as required by federal law. *See* 18 U.S.C. § 2258A(a). When Microsoft permanently suspends an account for sharing CSEAI and submits the required report to NCMEC, it does not tell the customer the basis for the account closure. This is so because in these circumstances, Microsoft does not know whether a civil or criminal investigation might arise and it cannot be complicit in the obstruction of justice. Davis Aff. ¶ 15. As a result, Microsoft notifies the user that he has violated the MSA and/or Code of Conduct, and due to the nature of the violation, the user will not be provided with further information. *Id.* Moreover, consistent with the MSA, Microsoft will not return any data from the OneDrive account to the user. *Id.* This data may be evidence of a potential criminal matter under investigation and Microsoft cannot be certain the OneDrive account does not contain other, undetected CSEAI. *Id.* This means returning the data to the customer carries the risk of Microsoft distributing CSEAI, which would violate federal law. *Id.*; *see also* 18 U.S.C. §§ 2251-2252.

c. Claimant's Microsoft Account, Purchase of Microsoft Services, and the MSA.

Claimant created a Microsoft account at least as early as 2013 using the email address tomdeutsch@aol.com. *See* Affidavit of Keith Walsh ("Walsh Aff.") ¶ 2. He admits he bought and used OneDrive, a cloud-storage service, and Microsoft 365 Personal ("M365 Personal"), which provides access to various Microsoft services, including increased OneDrive storage,⁵ through the Apple application ("app") store beginning in October 2019. Amended Claim at p. 1. To do so, he was first required to log into his Microsoft account on his Apple device, which allowed him to access his OneDrive through the OneDrive app for iOS. *See* Affidavit of Lauren Khoo ("Khoo Aff.") ¶ 2. When he logged into his Microsoft account on his Apple device, he had the opportunity to review the MSA in full by clicking on the hyperlink "Terms of use." *Id.* ¶¶ 3-4,

⁵ M365 Personal offers premium OneDrive features, including, among other services, increased cloud storage capacity. *See* [Microsoft 365 Plans \(Formerly Office 365\) - Microsoft Store](#). Under the MSA, customers may use M365 Personal services (including OneDrive) only for "personal, noncommercial use, unless [a user has] commercial use rights under a separate agreement with Microsoft." Davis Aff. Ex. A, MSA ¶ 14(i).

Exs. B-C. Once he was in his OneDrive, he had the option to buy an M365 Personal subscription using his iTunes account, as Claimant alleges he did here. *Id.* at Ex. D; Amended Claim at p. 1. Thus, when Claimant logged into his Microsoft account to purchase OneDrive and M365 Personal, and each time he logged in after to access and use those services, he was notified that “Terms of use” applied and had the opportunity to review those terms (the MSA) in full.⁶

The MSA expressly covers OneDrive and M365 Personal, and both require the customer to create a Microsoft Account before the customer may access the services—all of which Claimant did here. *See* Walsh Aff. ¶ 3; Khoo Aff. ¶ 2; Davis Aff. Ex. A, MSA (Covered Services). As the MSA states in its introductory paragraph: “You accept these Terms by creating a Microsoft account, through your use of the Services, or by continuing to use the Services after being notified of a change to these Terms.” Davis Aff. Ex. A, MSA (Introduction); *see also* Walsh Aff. ¶ 3.⁷

Consistent with this express language, Microsoft has periodically updated the MSA over the years, including as recently as 2019 and 2020. Walsh Aff. ¶ 4. Since 2014, it has provided notification to customers by email of these amendments, including providing in those notification emails a hyperlink to the amended terms so the customer may review them. *Id.* ¶¶ 4-5, Ex. A. In addition, in these email notifications Microsoft has informed customers that continued use of the Services after the effective date of the amended terms will be deemed an acceptance of the updated terms. *Id.* ¶¶ 4-5, Ex. A. By maintaining his Microsoft account and using OneDrive and M365 Personal, including after Microsoft’s email notice of amendments and after having opportunities to review the terms, Claimant has accepted the MSA, which governs his use of OneDrive and M365 Personal. *See id.* ¶¶ 3-6; Davis Aff. Ex. A, MSA (Covered Services).

d. Microsoft’s Detection of CSEAI Shared or Made Public from Claimant’s Account.

On May 12, 2020, Microsoft’s PhotoDNA technology detected and flagged as CSEAI an image shared or made public via OneDrive by the Microsoft account associated with the

⁶ When a customer buys an M365 Personal subscription via the Apple app store, as Claimant did here, the customer is shown the “Subscription Details.” Khoo Aff. Ex. E. As those “Subscription Details” explain, the purchase is through the customer’s “iTunes account”—which is an Apple account, not a Microsoft one. *Id.* The customer is also informed: “[t]o manage your subscriptions or to disable auto-renewal, after purchase, go to your iTunes account settings.” *Id.* (emphasis added); *see also id.* at Ex. D (showing customers buying subscriptions via the Apple app store are notified they can “[c]ancel anytime in Settings > Apple ID at least a day before each renewal date”). Claimant’s own exhibits confirm that his billing arrangement for the M365 Personal subscription is with Apple, not Microsoft. *See* Amended Claim at Ex. 1. Claimant does not deny that he could cancel his subscription through his Apple iTunes account. *See Id.* at I.

⁷ *See also* [Microsoft Services Agreement](#).

EXCERPTED EXHIBIT 9

AMERICAN ARBITRATION ASSOCIATION

THOMAS DEUTSCH, ESQ.,

Claimant,

v.

MICROSOFT CORPORATION,

Respondent.

:
:
:
:
:
:
:
:
:
:

CASE NO. 01-20-0014-3715

**AFFIDAVIT OF SEAN DAVIS IN SUPPORT
OF RESPONDENT MICROSOFT CORPORATION'S OPPOSITION TO MOTION FOR
PRELIMINARY INJUNCTION**

I, Sean Davis, hereby declare:

1. I am the Head of Digital Safety Operations at Microsoft Corporation ("Microsoft").

In this role, I am responsible for managing the team that reviews content detected or reported as child sexual exploitation and abuse imagery ("CSEAI"). Through my role and responsibilities, I am familiar with the development and use of PhotoDNA by Microsoft, as well as Microsoft's related practices and procedures. This affidavit is based on my own personal knowledge, discussions with appropriate Microsoft personnel, and review of Microsoft business records kept in the ordinary course of business.

2. Microsoft has a long-standing commitment and legitimate business interest in child online protection. In Microsoft's experience, the direct and indirect costs resulting from the presence of such images on its services can be significant. For example, they can increase the volume of consumer complaints received by Microsoft and, potentially, cause substantial harm to Microsoft's image and reputation in the marketplace. Microsoft believes that its customers are entitled to safer and more secure online experiences that are free of images depicting child sexual abuse. For these reasons, Microsoft devotes resources and develops and deploys technology to protect children online, and invests in research to better understand and combat online child sexual

exploitation. Microsoft is also a member of WeProtect, a global alliance of technology companies and international organizations dedicated to ending the sexual exploitation of children online.

3. Microsoft has codified its commitment to protecting children online in the “Code of Conduct” provision of the Microsoft Services Agreement (“MSA”). A true and correct copy of the applicable MSA is attached hereto as **Exhibit A**. The Code of Conduct sets online community standards and, among other things, prohibits “do[ing] anything illegal,” “engag[ing] in any activity that exploits, harms, or threatens to harm children” and “publicly display[ing] or us[ing] the Services to share inappropriate content or material (involving, for example, nudity, [and] pornography...).” Exhibit A, MSA at ¶ 3. These terms are informed, in part, by Microsoft’s business interests in ensuring its services are not used to proliferate the exploitation and abuse of children. In the Code of Conduct, Microsoft expressly reserves the right to remove such content from its services, ban participants, and terminate services: “[i]f you violate these Terms, we may stop providing Services to you or we may close your Microsoft account.” *Id.* The MSA further states that once an account is closed, the user “won’t be able to retrieve [his] Content or Data once [his] account is closed”. *Id.* at ¶ 4(a)(iv)(2).

4. Microsoft enforces this Code of Conduct and seeks to fulfill its commitment to ensuring a safe online environment for its users by, among other things, using PhotoDNA. PhotoDNA is an industry-leading image-matching technology that Microsoft developed in collaboration with Dartmouth College to assist Microsoft in its efforts to find and remove child sexual abuse imagery from its online services.

5. PhotoDNA uses a mathematical algorithm to create a unique signature—similar to a fingerprint—for each digital image. It does this by adjusting the image to a standard size for processing; converting the image into black and white and breaking the image into sections; calculating a unique number to represent each section, and then placing all those numbers together to create a single code that uniquely represents that image. That code is a unique signature for the

digital image, which can be compared with the signatures of other images to find copies of the original image. The technology can be used to find copies of a given image with incredible accuracy and at scale across the 1.8 billion images shared online every day, even when the images themselves have been altered.

6. The technique described in the above paragraph is known as “hashing.” PhotoDNA’s robust hashing differs from other hashing technologies because the PhotoDNA signature is based on the essence of the image and not the specific electronic file containing the image. Therefore, if an image has been resized, recolored, saved in a different file format or otherwise similarly altered, PhotoDNA can still reliably identify copies of the image when other hashing technologies (that require every file characteristic to be precisely the same) could not.

7. Microsoft makes the PhotoDNA program available without charge to qualified organizations, since the use of this service contributes to Microsoft’s business goal of creating a safer online experience.

8. Microsoft uses PhotoDNA on several of its services, including OneDrive, to scan certain user-generated content against a database of hashes of known images of child sexual abuse which have been identified by the National Center for Missing and Exploited Children (“NCMEC”) and Microsoft as the “worst of the worst” child pornography images.

9. To balance the privacy of its customers against the company’s legitimate business interest in ensuring safe services, PhotoDNA only becomes operative when images are shared or made public from a customer account. Microsoft does not search its customers’ private files. It is only when a customer shares an image from his or her OneDrive account, or makes an image from his or her OneDrive account public, that PhotoDNA is triggered.

10. Each image flagged by PhotoDNA has been subjected to additional human review by Microsoft to confirm that the image is, in fact, CSEAI. If there is any question as to whether an image is CSEAI or not, it will not be marked as such.

11. If the hash of scanned content matches the hash of a known image of child sexual abuse (also known as a “hit”), Microsoft takes several steps to prevent the continued access to and/or transmission of the images, to protect its customers, and to report the images as required by law. First, under the Code of Conduct, Microsoft suspends the account, such that the customer no longer has access to or use of the account or any other Microsoft online services associated with the account. Second, as required by federal law, Microsoft files a CyberTipline report with NCMEC. *See* 18 U.S.C. § 2258A.

12. Microsoft’s business records confirm that on May 12, 2020, PhotoDNA detected and flagged an image shared via OneDrive by the tomdeutsch@aol.com email account as CSEAI. The image was also subjected to human review by Microsoft to confirm that it was CSEAI. The image was confirmed as CSEAI classification A1 (a sex act involving a pre-pubescent child).

13. Because sharing CSEAI from OneDrive is a violation of the Code of Conduct, and because Microsoft detected and confirmed CSEAI shared from the OneDrive account for tomdeutsch@aol.com, Microsoft permanently suspended that account under the MSA.

14. On May 12, 2020, Microsoft filed CyberTipline report No. 72159146 with NCMEC to report the image match. Attached hereto as **Exhibit B** is a true and correct copy of the NCMEC Summary of CyberTipline Report.

15. Following the permanent suspension of an account based on a violation of the Code of Conduct, and particularly where a NCMEC report has been submitted, if an individual inquires into the reason for the suspension, Microsoft will not provide the reason for the account suspension. This is so because once Microsoft submits the CyberTipline report, it does not know whether a civil or criminal investigation might arise and cannot be complicit in obstruction of justice. Rather, Microsoft notifies the user that he has violated the MSA and/or Code of Conduct, and due to the nature of the violation, the user will not be provided with further information. Moreover, consistent with the MSA, Microsoft does not return any data from the OneDrive

account back to the user. This data may be evidence of a potential criminal matter under investigation and Microsoft cannot be certain the OneDrive account does not contain other CSEAI, creating the risk that returning the data in the OneDrive will result in Microsoft distributing CSEAI.

I declare under penalty of perjury under the laws of the State of New Jersey that the foregoing is true and correct to the best of my knowledge.

Executed on this 21st day of December, 2020 in Kirkland, WA.

A handwritten signature in cursive script that reads "Sean M. Davis".

Sean Davis

EXHIBIT 10

From: Harriet Derman <hderman@newjerseylaw.net>
Sent: Wednesday, January 13, 2021 2:13 PM
To: TOM DEUTSCH; Nahabet, Natalie; Shapiro, Marc R.; AAA Jenna Pascale
Subject: Status

A hearing with respect to Claimant's application for a preliminary junction was conducted today. Ms. Nahabet will furnish me with a form or Order, denying the application. Mr. Duetsch has indicated that he intends to hire counsel. He shall apprise us when he has done so. A conference shall be conducted on February 4, 2021 at 4:00 pm at which time hopefully with the addition of Mr.Deutsch's counsel the Report of Preliminary Hearing and Management Order can be completed. Judge Derman

EXHIBIT 11

From: Jason Lampert <jlampert@slwlawoffices.com>
Sent: Tuesday, February 9, 2021 12:38 PM
To: hderman@newjerseylaw.net; Shapiro, Marc R.; Nahabet, Natalie; JennaPascale@adr.org
Cc: Frank Salzano; Brady Williamson; Efthimios Parasidis
Subject: Thomas Deutsch, Esq. v. Microsoft Corporation - Case 01-20-0014-3715
Attachments: Deutsch Notice of Appearance of Counsel 2.9.2021.pdf

Dear Judge Derman, Mr. Shapiro, Ms. Nahabet and Ms. Pascale:

Please be advised that our firm was retained this afternoon to represent Thomas Deutsch in connection with the above-referenced arbitration. Enclosed please find our firm's notice of appearance.

Kind regards,

Jason Lampert
Salzano, Lampert & Wilson, LLP
275 Madison Avenue, 35th Floor
New York, NY 10016
Telephone: (646) 863-1883
Facsimile: (646) 365-3119
www.slwlawoffices.com

NOTICE: This message and its attachments are sent from a law office and may contain information that is confidential and protected by privilege from disclosure. If you are not the intended recipient, you are prohibited from printing, copying, forwarding or saving them. Please delete the message and attachments without printing, copying, forwarding or saving them, and notify the sender immediately.

Disclosure under IRS Circular 230: To ensure compliance with requirements imposed by the IRS, we inform you that any tax advice contained in this communication (including any attachments) was not intended or written to be used, and may not be used, for the purpose of avoiding tax-related penalties under federal, state or local tax law or promoting, marketing or recommending to another party any transaction or matter addressed therein.

EXHIBIT 12

From: Harriet Derman <hderman@newjerseylaw.net>
Sent: Wednesday, February 10, 2021 1:33 PM
To: AAA Jenna Pascale; Nahabet, Natalie; Shapiro, Marc R.; cc: Frank Salzano; Efthimios Parasidis; jlambert@slwlawoffices.com
Subject: Deutsch v. Microsoft

Dear Ms. Pascale,

I had a preliminary conference with counsel for defendants and plaintiff's new counsel to discuss the Preliminary Order. Counsel will work on completion of the Order and send me their draft by February 23. We shall have a conference call on February 24, 2021 at 4:00 PM. Can you send a call in number please.? Also, the Hearing was scheduled for August 2, 2021. I have a feeling it will take two days. Thank you. Harriet Derman

EXHIBIT 13

AMERICAN ARBITRATION ASSOCIATION

THOMAS DEUTSCH, ESQ.,

Claimant,

CASE NO. 01-20-0014-3715

v.

MICROSOFT CORPORATION,

Respondent.

**REPORT OF PRELIMINARY HEARING AND
SCHEDULING ORDER NO. 1**

Pursuant to the Consumer Arbitration Rules of the America Arbitration Association (“AAA”), a preliminary hearing was conducted by telephone in this matter on **February 10, 2021** (the “Hearing”), before Arbitrator, Honorable Harriet Derman, J.S.C. The counsel listed below appeared at the Hearing.

By Agreement of the parties and Order of the Arbitrator, the following is now in effect:

1. **Parties and Counsel.** The parties to this Arbitration are identified in the caption and represented as follows:

Counsel for Thomas Deutsch, Esq.

Frank C. Salzano, Esq.
Salzano, Lampert & Wilson, LLP
275 Madison Avenue, 35th Floor
New York, NY 10016

Counsel for Microsoft Corporation

Natalie Nahabet, Esq.
Orrick, Herrington & Sutcliffe, LLP
777 South Figueroa Street, Suite 3200
Los Angeles, CA 90017

Marc R. Shapiro, Esq.
Orrick, Herrington & Sutcliffe, LLP
51 West 52nd Street
New York, NY 10019

2. Arbitrator:

Honorable Harriet Derman, J.S.C.
c/o Olsen
521 Putting Green
Longboat Key, FL 34228
Email: hderman@newjerseylaw.net

**A new address will be provided for service of documents after March 25, 2021.*

3. AAA Case Administrator:

Jenna Pascale
Direct Dial: (401) 406-7095
Email: jennapasale@adr.org

No party shall have *ex parte* communications with the Arbitrator. Any documents and written communications directed to the Arbitrator or to the AAA shall be sent via e-mail to hderman@newjerseylaw.net and jennapasale@adr.org. All such correspondence shall also be simultaneously provided via email to the other party or parties to the arbitration.

Notwithstanding the foregoing, a hard copy of any documents exceeding ten (10) pages in length shall be sent by regular mail to the Arbitrator at the above address.

4. **Consent to the Arbitration and the Arbitrator:** Each of the parties, through counsel, confirmed that they consent, and have no objections, to Hon. Harriet Derman, J.S.C., serving as the Arbitrator in this matter.
5. **The Applicable Agreement to Arbitrate:** The parties agree that this matter is being arbitrated pursuant to the Microsoft Services Agreement, dated August 30, 2019 (the “MSA”).
6. **The AAA Procedural Rules:** Pursuant to the MSA and the agreement of the parties, this arbitration is governed by the Consumer Arbitration Rules of the AAA, Effective September 1, 2014 (the “AAA Consumer Rules”), https://www.adr.org/sites/default/files/Consumer_Rules_Web_0.pdf.
7. **Pleadings:** This Arbitration commenced pursuant to a Demand for Arbitration (“Demand”), submitted by Claimant on **August 14, 2020**. Claimant filed an Amendment thereto on **December 10, 2020**. Respondent answered the above on **September 15, 2020** and **December 23, 2020** respectively.
8. **The Applicable Law:** Pursuant to the MSA and the agreement of the parties, this Arbitration is governed by the substantive law of New Jersey and the Federal Arbitration Act.
9. **Preliminary Hearing(s).** An additional preliminary hearing has been set for **February 24, 2021 at 4:00 PM, Eastern Time**. Any subsequent preliminary hearings shall be held if needed, by

mutual agreement of the parties.

10. Amendments to Pleadings. Pursuant to the direction of the Arbitrator, all parties shall amend/specify claims and/or counterclaims and file any motion to join additional parties by **March 8, 2021**. Any answer to such amended claims or counterclaims shall be filed by **March 19, 2021**.

11. Discovery Schedule. Pursuant to the direction of the Arbitrator, the parties shall be allowed: ten (10) interrogatories, ten (10) document requests, and three (3) depositions of no longer than six-hours each. The following Discovery Schedule shall apply:

- | | |
|---|----------------|
| <input type="checkbox"/> Initial Document Requests and Interrogatories: | 3/12/21 |
| <input type="checkbox"/> Responses to Initial Document Requests and Interrogatories: | 4/2/21 |
| <input type="checkbox"/> Supplemental Document Requests and Interrogatories: | 4/9/21 |
| <input type="checkbox"/> Responses to Supplemental Document Requests and Interrogatories: | 4/30/21 |
| <input type="checkbox"/> Close of Fact Discovery: | 5/20/21 |

Claimant shall file his Motion to Compel production of the CSEAI image by **March 26, 2021**. Microsoft shall have until **April 16, 2021** to file its opposition. Claimant shall have until **April 23, 2021** to reply. Oral argument on the motion to compel will be heard on **May 4, 2021 at 4 pm ET**.

12. Subpoenas. Pursuant to AAA Consumer Rule 34(d), witnesses and/or documents may be subpoenaed by the Arbitrator or any other person authorized by law to do so upon the request of any party. A copy of such request shall be provided to the opposing party at the same time it is provided to the Arbitrator.

13. Witness Disclosures and Expert Reports

a) Pursuant to the direction of the Arbitrator, Claimant shall serve and file a disclosure of all witnesses reasonably expected to be called by the Claimant(s) on or before **May 24, 2021**.

b) Pursuant to the direction of the Arbitrator, Respondent shall serve and file a disclosure of all witnesses reasonably expected to be called by the Respondent(s) on or before **June 4, 2021**.

c) Disclosures shall include the full name of each witness, a short summary of anticipated testimony, copies of any expert reports, and written C.V. of experts. If certain required information is not available, the disclosures shall so state. Each party shall be responsible for updating its disclosures as such information becomes available. The duty to update this information continues up to and including the date that hearing(s) in this matter terminate.

14. Post-Discovery Conference Call. The parties and the Arbitrator will hold a status conference on **June 28, 2021 at 4 pm ET**, and will address on the call any procedural issues for the conduct of the Hearing, including whether written witness statements will replace any direct testimony at the Hearing.

- 15. Resolution of Discovery Disputes:** If the parties have any disputes relating to discovery issues, they shall attempt to resolve them and, if they are unable to do so, they shall promptly contact each other and the Arbitrator, via e-mail, as follows: (1) the party seeking a ruling shall set forth a short and plain summary of that party's position on each disputed item, along with an explanation of the efforts made to resolve the issue(s) with the counterpart; and (2) within five (5) calendar days thereafter the counterpart shall set forth a short and plain response. The Arbitrator shall notify the parties if and when she wishes to schedule a telephone conference to discuss the disputed issue(s).
- 16. Dispositive Motion(s).** Pursuant to the direction of the Arbitrator, Respondent, Microsoft Corporation may file its dispositive motion asserting immunity under Communications Decency Act § 230 on or before **June 11, 2021**. Claimant shall have until **June 28, 2021**, whichever is later, to respond. Microsoft shall have until **July 9, 2021**, to reply. No other dispositive motion shall be filed without the permission of the Arbitrator.
- 17. Exhibits**
- a) Not later than **July 20, 2021** the parties shall exchange copies of (or, when appropriate, make available for inspection) all exhibits to be offered and all schedules, summaries, diagrams and charts to be used at the Hearing. Each proposed exhibit shall be pre-marked for identification using the following designations:

PARTY	EXHIBIT # to #
_____	_____
_____	_____
_____	_____
_____	_____

- b) The parties shall attempt to agree upon and submit a jointly prepared consolidated and comprehensive set of joint exhibits.
- 18. Pre-Hearing Briefing:** The parties shall submit pre-hearing arbitration briefs by **July 27, 2021**.
- 19. Hearing.** The Hearing in this matter will commence before the Arbitrator at **10:00 AM, Eastern Time** on **August 2, 2021**. The parties estimate that this case will require **two (2) days** of hearing time, inclusive of arguments. The Hearing shall be conducted via Zoom videoconference.
- 20. Post-Hearing Briefing:** The parties shall submit post-hearing arbitration briefs by **August 23, 2021**.
- 21. Deadlines.** All deadlines stated herein will be strictly enforced. After such deadline, the parties may not file such motions except with the permission of the Arbitrator, good cause having been shown.
- 22. Award:** The Arbitrator will issue a written award, which shall include a reasoned and detailed decision stating the reasons upon which it is based and supported by essentials facts and conclusions of law.

23. **Court Reporter:** The parties agree that the Hearing shall be transcribed, and the costs of such shall be split equally between the parties.

24. **Objections:** In the event the parties disagree with or otherwise object to anything stated in this Order, they shall so inform the Arbitrator within seven (7) days of receipt of this Order.

This order shall continue in effect unless and until amended by subsequent order of the Arbitrator.

SO ORDERED:

Dated: _____

Honorable Harriet Derman, J.S.C
Arbitrator

23. **Court Reporter:** The parties agree that the Hearing shall be transcribed, and the costs of such shall be split equally between the parties.

24. **Objections:** In the event the parties disagree with or otherwise object to anything stated in this Order, they shall so inform the Arbitrator within seven (7) days of receipt of this Order.

This order shall continue in effect unless and until amended by subsequent order of the Arbitrator.

Dated: _____

2/24/21.

SO ORDERED:

Honorable Harriet Derman, J.S.C
Arbitrator

EXHIBIT 14

AMERICAN ARBITRATION ASSOCIATION

THOMAS DEUTSCH, ESQ.,

Claimant,

CASE NO. 01-20-0014-3715

v.

MICROSOFT CORPORATION,

Respondent.

**CLAIMAINT'S MOTION TO COMPEL
PRODUCTION OF ALLEGED CSEAI**

TABLE OF CONTENTS

Table of Contents.....2

Table of Authorities.....3

Introduction.....4

Argument.....5

 I. Legal Standard.....5

 II. The Arbitrator Should Compel Production Of The Alleged CSEAI Because It
 Is The Key Document That Is Central To Resolution Of This Arbitration.....5

 III. Production Of The Alleged CSEAI Is Not Categorically Precluded By Law.....6

 IV. The Arbitrator Has The Discretion To Compel Production For Limited Review.....8

 V. Insofar As The Alleged CSEAI Is Not Produced, Respondent Should Be
 Precluded From Relying Upon The Alleged CSEAI In Its Defense Of
 This Arbitration9

Conclusion.....9

TABLE OF AUTHORITIES

CASES

Bell v. Lockheed Martin Corp., 270 F.R.D. 186 (D.N.J. 2010), *aff’d*, 2010 WL 3724271 (D.N.J. Sept. 15, 2010).....5, 6

State National Insurance Co. v. County of Camden, 2011 WL 13079217 (D.N.J. April 28, 2011)6

G.A.-H v. K.G.G., 189 A.3d 906 (N.J. App. Div. 2018), *rev’d on other grounds*, 238 N.J. 401 (2019).....7, 8

State v. Scoles, 214 N.J. 236 (N.J. 2013).....7, 8

Wagner v. Blue Sky Classic Cars L.L.C., 2012 WL 5381720 (N.J. App. Div. Nov. 5, 2012)9

Hibbert v. Bellmawr Park. Mut. Housing Corp., 2013 WL 3949024 (D.N.J. Aug. 1, 2013)9

STATUTES

18 U.S.C. § 3509(m)(1)7

OTHER AUTHORITIES

N.J. Ct. R. R. 4:10-25, 6

INTRODUCTION

This motion seeks to compel production of the single piece of evidence that is integral and essential to the just, equitable, and prompt resolution of this arbitration. Claimant Thomas Deutsch (hereinafter “Claimant”) filed this arbitration against Respondent Microsoft Corporation (hereinafter “Microsoft” or “Respondent”) because Microsoft wrongfully closed Claimant’s OneDrive account, Microsoft wrongfully precluded Claimant from accessing his files stored on OneDrive, and Microsoft wrongfully confiscated thousands of Claimant’s documents that are stored on OneDrive. Microsoft asserts the sole reason for its conduct is that Microsoft’s computer program, PhotoDNA, allegedly flagged a single image that Claimant shared via OneDrive that Microsoft asserts is illegal child pornography.

This alleged image, which Microsoft characterizes as illegal child sexual exploitation and abuse imagery (hereinafter “CSEAI”), has not been reviewed by counsel for Microsoft, has not been independently verified as CSEAI by a third party, has not been shared with the Arbitrator in this matter, and has not been produced to Claimant or Claimant’s counsel. Moreover, although Microsoft shared a copy of the alleged illegal CSEAI with federal law enforcement officials on May 12, 2020, as of the date of this motion, no law enforcement official has contacted Claimant. The absence of law enforcement inquiry into the matter strongly suggests that the image was not, in fact, illegal CSEAI. Nevertheless, Microsoft has informed Claimant and the Arbitrator that the company will not produce the alleged CSEAI absent an order from the Arbitrator in this matter.

For the reasons outlined herein, Claimant respectfully requests that the Arbitrator compel production of the alleged CSEAI. Additionally, insofar as Microsoft does not produce the alleged

CSEAI, Claimant respectfully requests that the Arbitrator rule that Microsoft is precluded from utilizing the alleged CSEAI in its defense of the claims brought in this arbitration.

ARGUMENT

I. Legal Standard

Pursuant to New Jersey Rules of Court 4:10-2(a), “parties may obtain discovery regarding any matter, not privileged, which is relevant to the subject matter involved in the pending action, whether it relates to the claim or defense of the party seeking discovery or to the claim or defense of any other party.” N.J. Ct. R. R. 4:10-2. Moreover, “the Court may . . . permit for ‘good cause’ discovery of matters that are ‘relevant to the subject matter involved in the action.’” *See Bell v. Lockheed Martin Corp.*, 270 F.R.D. 186, 191 (D.N.J. 2010), *aff’d*, 2010 WL 3724271 (D.N.J. Sept. 15, 2010) (citations omitted).

As New Jersey courts have further held, “[o]n a motion to compel discovery or for a protective order, the party from whom discovery is sought shall demonstrate that the information is not reasonably accessible because of undue burden or cost. If that showing is made, the court nevertheless may order discovery from such sources if the requesting party establishes good cause, considering the limitations of R. 4:10-2(g). The court also may specify conditions for the discovery.” N.J. Ct. R. R. 4:10-2.

II. The Arbitrator Should Compel Production Of The Alleged CSEAI Because It Is The Key Document That Is Central To Resolution Of This Arbitration

The alleged CSEAI is a central piece of evidence in this arbitration. Microsoft terminated Claimant’s OneDrive account, precluded Claimant from accessing his files stored on OneDrive, and confiscated thousands of Claimant’s documents because, Microsoft claims, the

company found a CSEAI image that Claimant allegedly shared via OneDrive. In short—Microsoft’s actions, and much of this entire arbitration—revolve around one image and whether Microsoft took reasonable steps in identifying the image as CSEAI and acting in a reasonable manner following that identification.

Without proof that the image is, in fact, CSEAI, Microsoft’s defense completely unravels. If—as Claimant contends—the image is not CSEAI, then Microsoft has breached its agreement with Claimant and has otherwise engaged in wrongful and illegal conduct. Moreover, Claimant will be unable to prosecute this matter without the ability to review the alleged CSEAI. The image is, without question, a key—if not *the* key—piece of evidence in this arbitration.

As New Jersey courts have consistently recognized, a party may obtain discovery regarding any nonprivileged matter that is relevant to a party’s claim or defense. *See Bell*, 270 F.R.D. at 191 (citations omitted). And, “relevancy is more liberally and broadly construed at the discovery stage than at trial.” *State National Insurance Co. v. County of Camden*, 2011 WL 13079217, at *3 (D.N.J. April 28, 2011) (citations omitted). Here, there can be no serious question on the relevancy of the image to the just, equitable, and prompt resolution of this matter. Because the image is a key piece of evidence, Claimant respectfully requests that the Arbitrator compel production.

III. Production Of The Alleged CSEAI Is Not Categorically Precluded By Law

Production of the alleged CSEAI is not categorically precluded by law. During a conference call regarding this arbitration that included the Arbitrator and counsel for Claimant and Respondent, counsel for Microsoft alleged that federal law precludes Respondent from producing the image that is allegedly CSEAI, a position that Microsoft repeated in its Answer to the Third Amended Claim. However, contrary to Microsoft’s position, federal or state law does

not categorically preclude production of the alleged CSEAI. Rather, New Jersey law *permits* disclosure of child pornography where—as here—a just resolution necessitates access and review of the alleged CSEAI.

In federal criminal matters, “any property or material that constitutes child pornography shall remain in the care, custody, and control of either the Government or the court.” 18 U.S.C. § 3509(m)(1). Where alleged CSEAI is central to a case, New Jersey courts have compelled production of the images in *both civil and criminal matters*. See e.g., *G.A.-H v. K.G.G.*, 189 A.3d 906, 909-910 (N.J. App. Div. 2018), *rev’d on other grounds*, 238 N.J. 401 (2019); *State v. Scoles*, 214 N.J. 236, 254 (N.J. 2013) (citations omitted).

As the New Jersey Supreme Court has recognized, “[d]iscovery disputes involving an accused’s access to computer images of alleged child pornography require a consistent approach.” *Scoles*, 214 N.J. at 245-246. This involves balancing the need for parties to have access to evidence that permits the fair adjudication of claims with the public policy of not facilitating the distribution of child pornography. See *id.* The New Jersey Supreme Court has struck this balance in a reasonable manner, by permitting compelled production of alleged CSEAI in conjunction with a protective order that details a limited group of individuals that is permitted access to the alleged CSEAI. See *id.*

Importantly, in New Jersey, compelled production of alleged CSEAI is not limited to criminal matters. For example, in the civil case of *GA-H vs. K.G.G.*, a New Jersey appellate court overturned a trial court’s decision not to require “a turnover or even an in-camera review of materials gathered by the prosecutor during a criminal investigation” that led to the defendant’s conviction in a prior criminal case. *G.A.-H*, 189 A.3d at 909-910. Highlighting the “significance of this evidence” to the civil matter, *id.* at 909 n.5, the court compelled production of the child

pornography pursuant to a protective order that limited review of the evidence. *See id.* at 909-910. The court further ruled that the turnover of the evidence pursuant to a protective order did not amount to violation of a New Jersey law that criminalizes receipt of child pornography. *See id.*

Taken together, it is clear that New Jersey law does not categorically preclude production of CSEAI. Moreover, New Jersey has taken the position that compelled production of alleged CSEAI is appropriate so long as the Arbitrator balances the applicable public policy concerns. For these reasons, Claimant respectfully requests that the Arbitrator compel production of the image.

IV. The Arbitrator Has The Discretion To Compel Production For Limited Review

As detailed in Section III of this Motion to Compel, the Arbitrator maintains great flexibility to compel production of the alleged CSEAI for limited review via a protective order. This is appropriate here, where the sole image at issue allegedly contains CSEAI and counsel for Claimant and Microsoft have yet to review the image despite this dispute originating nearly a year ago. Limited review of the alleged CSEAI will facilitate the just, equitable, and prompt resolution of this arbitration. This is particularly true here, where Claimant vehemently denies that he possessed or shared CSEAI and law enforcement authorities have taken no measures against Claimant despite being on notice of the alleged CSEAI for nearly one year.

With respect to the alleged CSEAI in this matter, the Arbitrator can grant limited review of the alleged CSEAI solely for the Arbitrator herself, counsel for Claimant and Respondent, and for an independent review by a third party to issue an expert opinion as to whether the image qualifies as CSEAI. The Arbitrator then could issue a protective order regarding such production that expressly limits review of the alleged CSEAI solely for this arbitration. Protective orders

have been utilized in civil and criminal cases involving alleged CSEAI and related images. *See e.g., G.A.-H*, 189 A.3d at 909-910; *Scoles*, 214 N.J. at 254 (citations omitted). This limited review serves to balance the public policy goal against distribution of child pornography with the public policy goal of facilitating the just, equitable, and prompt resolution of claims.

V. Insofar As The Alleged CSEAI Is Not Produced, Respondent Should Be Precluded From Relying Upon The Alleged CSEAI In Its Defense of this Arbitration

If Microsoft does not produce the alleged CSEAI, Microsoft should be precluded from relying upon the image in its defense during this arbitration. It is axiomatic that factual evidence not produced during discovery cannot be used in the prosecution or defense of a claim or defense. *See, e.g., Wagner v. Blue Sky Classic Cars L.L.C.*, 2012 WL 5381720, at *4 (N.J. App. Div. Nov. 5, 2012) (holding that documents not produced during discovery could not be utilized during trial). This rule has been established to promote fairness and equipoise in the prosecution and defense of both civil and criminal matters, and is essential to just and equitable adjudication of arbitrations.

Microsoft has justified its actions in this matter—terminating Claimant’s OneDrive account, precluding Claimant from accessing his documents stored on OneDrive, and confiscating thousands of Claimant’s files—because it allegedly found a single CSEAI image that Claimant allegedly shared via OneDrive. It belies fundamental principles of justice and fairness to allow Microsoft to use the image as both a sword and a shield. *See, e.g., Hibbert v. Bellmawr Park. Mut. Housing Corp.*, 2013 WL 3949024, at *3 (D.N.J. Aug. 1, 2013) (indicating that a party “should not benefit from his failure to timely produce relevant discovery”).

For the foregoing reasons, Claimant respectfully requests that the Arbitrator order that Microsoft produce the image, and thus have the ability to use the image in its defense. But,

insofar as Microsoft does not produce the image, Claimant respectfully requests that Microsoft be precluded from utilizing the image in its defense.

CONCLUSION

For the reasons outlined herein, Claimant respectfully requests that the Arbitrator compel production of the alleged CSEAI. Additionally, insofar as Microsoft does not produce the alleged CSEAI, Claimant respectfully requests that the Arbitrator rule that Microsoft is precluded from utilizing the alleged CSEAI in its defense of the claims brought in this arbitration.

Dated: March 26, 2021

SALZANO, LAMPERT & WILSON, LLP

By: /s/ Frank Salzano

Frank Salzano, Esq. (NY SBN 4114849)
275 Madison Avenue, 35th Floor
New York, New York 10016
(646) 863-1883
fsalzano@slwlawoffices.com

Attorneys for Claimant

EXHIBIT 15

AMERICAN ARBITRATION ASSOCIATION

THOMAS DEUTSCH, ESQ.,

Claimant,

CASE NO. 01-20-0014-3715

v.

MICROSOFT CORPORATION,

Respondent.

**REPORT OF PRELIMINARY HEARING AND
SCHEDULING ORDER NO. 2**

On May 3, 2021, the parties appeared before Arbitrator, the Honorable Harriet Derman, J.S.C., for a scheduling conference. By Agreement of the parties and Order of the Arbitrator, the following schedule is now in effect:

1. **Supplement to Answer.** Microsoft shall submit its Supplement to the Answer to Claimant's Third Amended Claim on **May 10, 2021**.
2. **Motion to Compel.** Microsoft shall file its Opposition to Claimant's pending Motion to Compel production of the CSEAI image on **May 17, 2021**. Claimant shall file his reply on **May 28, 2021**.
3. **Section 230 Motion to Dismiss.** Microsoft shall file its Motion to Dismiss under Section 230 of the Communications Decency Act on **May 17, 2021**. Claimant shall file his opposition to the motion on **June 8, 2021**. Microsoft shall file its reply on **June 18, 2021**.
4. **Hearings on Motion to Compel and Section 230 Motion to Dismiss.** Claimant's Motion to Compel and Microsoft's Section 230 Motion to Dismiss shall be heard on **June 28, 2021 at 4 pm EST**.
5. **Discovery Schedule.** All discovery shall be stayed pending resolution of the Motion to Compel and Section 230 Motion to Dismiss. Thereafter, the responses to any Supplemental Document Requests and/or Interrogatories shall be due two weeks from the date of such requests. Fact discovery shall close on **July 30, 2021**.
6. **Witness Disclosures and Expert Reports**

a) Claimant shall serve and file a disclosure of all witnesses reasonably expected to be called by the Claimant on or before **July 16, 2021**.

b) Respondent shall serve and file a disclosure of all witnesses reasonably expected to be called by the Respondent on or before **July 30, 2021**.

c) Disclosures shall include the full name of each witness, a short summary of anticipated testimony, copies of any expert reports, and written C.V. of experts. If certain required information is not available, the disclosures shall so state. Each party shall be responsible for updating its disclosures as such information becomes available. The duty to update this information continues up to and including the date that hearing(s) in this matter terminate.

7. **Dispositive Motion(s)**. The parties may file simultaneous dispositive motions with opening briefs to be submitted on **August 6, 2021**. The opposing party shall file its opposition to the dispositive motion on **August 25, 2021**. The moving party shall file its reply on **September 3, 2021**. Oral argument on the parties' dispositive motions shall be heard on **September 15, 2021 at 12 p.m. EST**.

8. **Exhibits**

a) Not later than **September 28, 2021** the parties shall exchange copies of all exhibits to be offered and all schedules, summaries, diagrams and charts to be used at the Hearing.

b) The parties shall attempt to agree upon and submit a jointly prepared consolidated and comprehensive set of joint exhibits.

9. **Pre-Hearing Briefing**. The parties shall submit pre-hearing arbitration briefs by **October 5, 2021**.

10. **Hearing**. The Hearing in this matter will commence before the Arbitrator at **11:00 AM, Eastern Time on October 12, 2021**. The parties estimate that this case will require **1-2 days** of hearing time, inclusive of arguments. The Hearing shall be conducted via Zoom videoconference.

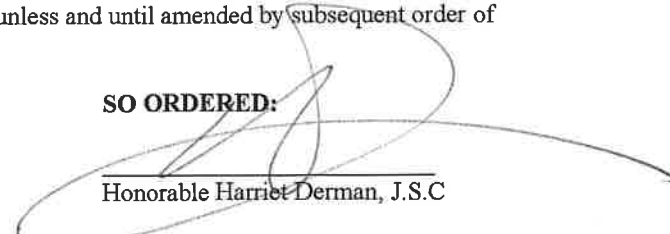
11. **Post-Hearing Briefing**. The parties shall submit post-hearing arbitration briefs by **November 2, 2021**.

12. **Scheduling Order No. 1**. All other provisions of the February 24, 2021 Scheduling Order not inconsistent with the above shall remain in effect.

This order shall continue in effect unless and until amended by subsequent order of the Arbitrator.

Dated: 5/7/21

SO ORDERED:


Honorable Harriet Derman, J.S.C.

**EXCERPTED
EXHIBIT 16**

AMERICAN ARBITRATION ASSOCIATION

THOMAS DEUTSCH, ESQ.,

Claimant,

v.

MICROSOFT CORPORATION,

Respondent.:
:
:
:
:
:
:
:
:
:
:
:

CASE NO. 01-20-0014-3715

RESPONDENT MICROSOFT CORPORATION'S SUPPLEMENT TO ITS ANSWER TO CLAIMANT'S THIRD AMENDED CLAIM

Respondent Microsoft Corporation submits the following supplemental answer to Claimant Thomas Deutsch's Third Amended Claim (the "Third Amended Claim") as follows:

1. Microsoft has previously explained in this litigation, including in its Answer to the Third Amended Claim, that PhotoDNA was only triggered in OneDrive when a customer shared an image with another person, or made an image accessible to others (such as by saving the image to a shared folder in OneDrive). Those statements were correct to the best of Microsoft's knowledge when Microsoft made them, and they accurately state Microsoft's practice to run PhotoDNA when a consumer shares an image or makes an image accessible to anyone else.

2. Recently, however, through investigating Exhibit 2 to the Third Amended Claim, Microsoft discovered that a "recap" feature in OneDrive, when "on" in a user's OneDrive account, identified some images in that user's OneDrive to "recap" for him or her, and when that happened, changed the status of the image to "shared," triggering PhotoDNA. That is, OneDrive's act of identifying an image to "recap" for the customer caused the status of that image to be in a "shared" state. Because the image was in a "shared" state, PhotoDNA was triggered to scan the image, regardless whether the customer had taken action to share the image with anyone else or save it to a shared folder. OneDrive did not, however, send the "recapped" image to anyone else; nor did OneDrive's act of recapping (or sharing) the image with that same customer make the image available to anyone else.

3. This "recap" feature had no impact on PhotoDNA's accuracy or Microsoft's human review process. The same PhotoDNA technology and human review process were employed regardless whether the "recap" feature, or the customer's act of sharing the image or saving it to a shared folder, caused PhotoDNA to scan the image.

4. Upon discovering how this "recap" feature was interacting with and triggering PhotoDNA, Microsoft investigated whether the feature could have caused the PhotoDNA scanning event in Claimant's case. Based on the preserved metadata for the image that PhotoDNA flagged from Claimant's OneDrive account, Microsoft was able to confirm that this "recap" feature had changed the status of this image to "shared," causing PhotoDNA to scan the image. Promptly

upon becoming aware that the “recap” feature caused PhotoDNA to scan the image here, Microsoft disclosed these details to Claimant’s counsel. Microsoft has also disabled the feature.

5. Microsoft now submits this supplemental answer to correct prior statements it has made in this arbitration that PhotoDNA only scanned content in OneDrive when the customer shared an image or saved it to a shared folder. This includes statements in Microsoft’s prior Answers, Microsoft’s Opposition to the Motion for Preliminary Injunction, the Affidavit of Sean Davis in Support of Microsoft’s Opposition to Motion for Preliminary Injunction, and any statements made by Microsoft’s counsel during hearings or oral argument.

6. Microsoft maintains that Claimant violated the Microsoft Services Agreement (MSA). The MSA’s Code of Conduct prohibits users from “engag[ing] in any activity that exploits, harms, or threatens to harm children,” or “engag[ing] in activity that violates the privacy of others.” *See* MSA §§ 3(a)(ii) & (ix). Here, and as Microsoft has previously disclosed, PhotoDNA and human review confirmed the image was CSEAI, in violation of MSA §§ 3(a)(ii) & (ix).

7. Microsoft complied with the MSA and its Privacy Statement (incorporated by reference into the MSA) when it scanned Claimant’s content to ensure the safety of its services, and when it closed the account upon detecting CSEAI. The Privacy Statement expressly provides for automated scanning of user data, regardless whether the data is private or shared. In the event an automated OneDrive scan results in a determination that a user is in possession of CSEAI, Microsoft is permitted to retain and/or access the user’s content, including the “content of ... files in private folders on OneDrive,” to enforce the terms of the MSA and protect customers. In particular, the Privacy Statement explains:

How we use personal data...

Safety. ... some of our products, such as ... OneDrive, systematically scan content in an automated manner to identify ... abusive actions ...; and we reserve the right to block delivery of a communication or remove content if it violates our terms.

...

Protecting rights and property. We use data to ... enforce [our] agreement, and protect our property.... We may use automated processes to detect and prevent activities that violate our rights and the rights of others....

...

Reasons we share personal data...

we will retain, access, transfer, disclose, and preserve personal data, including your content (such as the content of ... files in private folders on OneDrive), when we have a good faith belief that doing so is necessary to do any of the following: ...

- Protect our customers, for example, ... to help prevent the loss of life or serious injury of anyone....

- Protect the rights or property of Microsoft, including enforcing the terms governing the use of the services....

Exhibit A, Microsoft's Privacy Statement.

In addition, under the enforcement provision in the MSA's Code of Conduct, Microsoft states: "b. **Enforcement.** If you violate these Terms, we may stop providing Services to you or we may close your Microsoft account.... When investigating alleged violations of these Terms, Microsoft reserves the right to review Your Content in order to resolve the issue." MSA § 3.b; *see also id.* § 1 (defining "Your Content" as "the files, photos, documents, audio, digital works, livestreams and videos that you upload [or] store ... through the Services," which include OneDrive).

8. When Microsoft identified and confirmed CSEAI in Claimant's OneDrive and consequently, suspended Claimant's account, Microsoft acted consistent and in compliance with the plain terms of the MSA and Privacy Statement, neither of which limited Microsoft to scanning and reviewing only content a OneDrive user shares, or limited Microsoft's ability to suspend an account storing known CSEAI in a private folder.

9. Based on Claimant's violation of the Code of Conduct, Microsoft is entitled to maintain the block on Claimant's MSA account without returning the data in the account. *See* MSA §§ 3.a.ii & ix, 3.b., 4.iv.2. Likewise, Microsoft's decision to block Claimant's MSA account without returning the data upon detecting confirmed CSEAI in the account is entitled to litigation immunity under Section 230 and established case law. *See Domen v. Vimeo*, 991 F.3d 66, 68 (2d Cir. 2021) (Section 230(c)(2) granted Vimeo immunity from suit when it deleted user's *entire* account as opposed to only the content it deemed objectionable); *e360Insight, LLC v. Comcast Corp.*, 546 F. Supp. 2d 605, 609 (N.D. Ill. 2008) ("Under the law, [even] a mistaken choice to block, if made in good faith, cannot be the basis for liability under federal or state law."). Microsoft therefore maintains all defenses set forth in its Answer to the Third Amended Claim.

Dated: May 10, 2021

RESPONDENT MICROSOFT CORPORATION

By: /s/ Natalie Nahabet
 Marc R. Shapiro (NY SBN 4403606)
 Natalie Nahabet (CA SBN 301597)
 ORRICK, HERRINGTON & SUTCLIFFE LLP
 777 South Figueroa Street, Suite 3200
 Los Angeles, CA 90017
 Telephone: (213) 629-2020
 Facsimile: (213) 612-2499
 Email: mrshapiro@orrick.com
 nnahabet@orrick.com

ATTORNEYS FOR RESPONDENT MICROSOFT
 CORPORATION

EXCERPTED EXHIBIT 17

AMERICAN ARBITRATION ASSOCIATION

THOMAS DEUTSCH, ESQ.,	:	
	:	
<i>Claimant,</i>	:	CASE NO. 01-20-0014-3715
	:	
v.	:	
	:	
MICROSOFT CORPORATION,	:	
	:	
<i>Respondent.</i>	:	

RESPONDENT MICROSOFT CORPORATION’S
MOTION FOR JUDGMENT ON THE PLEADINGS TO
DISMISS THIRD AMENDED DEMAND UNDER
SECTION 230 OF THE COMMUNICATIONS DECENCY ACT

Table of Contents

I. INTRODUCTION 3

II. BACKGROUND..... 4

**a. Congress Enacted Section 230 to Protect Service Providers from Litigation
 Arising from Acts Taken to Maintain a Safe Online Experience..... 4**

**b. Microsoft Developed Standardized Protocols to Detect and Confirm CSEAI and
 Enforce Its Code of Conduct. 6**

**c. PhotoDNA Detected Material Confirmed by Human Review to be CSEAI in
 Claimant’s OneDrive..... 8**

III.LEGAL STANDARD 8

IV.ARGUMENT 10

a. Microsoft is an Interactive Computer Service. 10

**b. Microsoft Blocked Claimant’s Access to OneDrive and Suspended His Account
 Upon Detecting and Confirming CSEAI in the Account. 11**

**c. Microsoft Suspended Claimant’s Account in Good Faith, Upon Detecting and
 Confirming CSEAI in the Account. 11**

V. CONCLUSION 15

I. INTRODUCTION

The Arbitrator should dismiss the Third Amended Arbitration Demand with prejudice because it seeks to hold Microsoft liable for the very conduct Congress declared immune from suit: for detecting and blocking access to child sexual exploitation and abuse imagery on its services. Congress created this immunity in the Communications Decency Act (“CDA”) precisely to encourage internet service providers to stem the proliferation of child sexual abuse and exploitation imagery online. S. Rep. No. 104-23, at 59 (1995). The CDA accomplishes this by, among other things, granting internet service providers immunity from suit for “any action voluntarily taken in good faith to restrict access to ... material that the provider ... considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable....” 47 U.S.C. § 230(c)(2)(A). Microsoft’s actions here fall squarely within the CDA’s safe harbor.

On May 12, 2020, Microsoft detected child sexual exploitation and abuse imagery (“CSEAI”) in Claimant’s OneDrive account. CSEAI is, by its very nature, “obscene, lewd, lascivious, filthy, excessively violent, harassing, [and] otherwise objectionable.” Not surprisingly, in its Code of Conduct in the Microsoft Services Agreement (“MSA”), Microsoft expressly prohibits customers such as Claimant from using Microsoft’s services for CSEAI, requiring customers to agree they will not “engage in any activity that exploits, harms, or threatens to harm children.” Nahabet Declaration ISO Opposition to Motion to Compel (“Nahabet Decl.”), Exhibit A, (“MSA”), ¶ 3.a.ii. Because Microsoft detected CSEAI in Claimant’s account, it “restrict[ed] access to” the imagery by blocking his access to OneDrive and suspending his account.

And it did so in good faith. Microsoft relied on highly accurate (to the tune of 1 error in 50 billion), industry-leading, standardized PhotoDNA technology and human confirmation to detect and confirm the image as CSEAI. Microsoft took these actions under the plain terms of its Privacy Statement and Code of Conduct, both of which are part of the MSA between Claimant and Microsoft, and both of which allowed Microsoft to scan and review content in Claimant’s OneDrive to ensure the safety and security of Microsoft’s services. *See* MSA, ¶ 1 (“**Your Privacy**,” incorporating Privacy Statement) & ¶ 3 (“**Code of Conduct**”). Just as the Privacy Statement and Code of Conduct allowed Microsoft to detect and confirm CSEAI in Claimant’s OneDrive, so too did these terms expressly allow Microsoft to suspend Claimant’s OneDrive without returning the data in it to him as a result of that detection and confirmation. *Id.* at ¶ 3.b.

Because Microsoft acted in good faith in suspending Claimant’s OneDrive after detecting confirmed child sexual exploitation and abuse imagery in the account, Section 230(c)(2)(A) immunity applies, and the Arbitrator should grant judgment on the pleadings and dismiss the Third

Amended Demand with prejudice. *See Domen v. Vimeo, Inc.*, 991 F.3d 66, 71 (2d Cir. 2021) (affirming grant of motion to dismiss under Section 230 where service provider closed account for posting sexual orientation change effort videos in violation of provider’s terms).¹

II. BACKGROUND

a. Congress Enacted Section 230 to Protect Service Providers from Litigation Arising from Acts Taken to Maintain a Safe Online Experience.

Following a series of reports of a surge in online pornography, in 1995, Senator J. James Exon proposed legislation that later became known as the Communications Decency Act. Senator Exon explained his motivation for the legislation: “the information superhighway should not become a red light district. [The CDA] will keep that from happening and extend the standards of decency which have protected telephone users to new telecommunications devices.” 141 Cong. Rec. S1953 (daily ed. Feb. 1, 1995) (statement of Rep. Exon). It is now well-understood that the “[t]he primary purpose of the CDA was to protect children from sexually explicit content.” *Domen v. Vimeo, Inc.*, 991 F.3d 66, 71 (2d Cir. 2021) (quoting *FTC v. LeadClick Media, LLC*, 838 F.3d 158, 173 (2d Cir. 2016)) (internal quotations omitted).

Section 230 was designed to advance the CDA’s goals. At the time, plaintiffs’ lawyers were targeting computer service providers for actions (and inactions) taken (or not) with respect to hosted content. Companies thus feared the litigation risk that accompanied moderating content. *See Enigma Software Group USA, LLC v. Malwarebytes, Inc.*, 946 F.3d 1040, 1046 (9th Cir. 2019) (explaining that before the CDA, “once a service provider undertook to filter offensive content from its network, it assumed responsibility for any offensive content it failed to filter, even if it lacked knowledge of the content”).

Enter Section 230. The statute was designed to “encourage telecommunications and

¹ As discussed below, on this motion the Arbitrator may consider documents on which Claimant’s Third Amended Arbitration Demand relies or that are specifically referenced in that Demand. This includes the MSA, which Claimant references in the Demand and which incorporates the Privacy Statement (*see* MSA ¶ 1), as Claimant’s claims arise from his relationship with Microsoft, which the MSA and its terms (including the Privacy Statement and Code of Conduct) govern. *See* Section III, *infra*; Third Amended Demand at §§ II-V, pp. 5, 7-8, 11, 14-16. For the convenience of the Arbitrator, Microsoft cites the MSA and incorporated Privacy Statement that are attached as Exhibits A & B, respectively, to the Nahabet Declaration. For ease of review, Microsoft cites these directly, as MSA and Privacy Statement. The MSA attached as Exhibit A to the Nahabet Declaration is the same version of the MSA that Claimant attached to his original arbitration demand. *See* Claimant’s August 14, 2020 Arbitration Demand, p. 23 (incorporating Privacy Statement).

information service providers to deploy new technologies and policies ... to prevent the use of their systems or services for prohibited purposes.” S. Rep. No. 104-23, at 59 (1995). It did this through a quid pro quo: “in return for [Congress conferring upon computer service providers] th[e] protection ... that they wouldn’t be sued indiscriminately,” the providers were to be “responsible in terms of policing their platforms.” Alina Selyukh, *Section 230: A Key Legal Shield for Facebook, Google Is About to Change*, NPR (Mar. 21, 2018) (quoting Senator Wyden). As the statute’s own policy statement states, Congress enacted Section 230 “to remove disincentives for the development and utilization of blocking and filtering technologies that empower parents to restrict children’s access to objectionable or inappropriate online material,” and “to ensure vigorous enforcement of Federal criminal laws to deter and punish in trafficking in obscenity ... by means of computer.” 47 U.S.C. § 230(b)(4)-(5).

Section 230(c) of the Act effectuates this goal. As relevant here, that Section provides:

(2) Civil Liability

No provider ... of an interactive computer service shall be held liable on account of—

(A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider ... considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable....

47 U.S.C. § 230(c)(2)(A).

Courts have long agreed Section 230’s safe harbor immunity provisions should be “construed ... broadly” to fulfill Congress’s intent. *Jones v. Dirty World Entm’t. Recordings LLC*, 755 F.3d 398, 408 (6th Cir. 2014); *LeadClick*, 838 F.3d at 173 (same and collecting cases). Indeed, “[t]he legislative history demonstrates Congress intended to extend immunity to *all* civil claims.” *Doe II v. MySpace Inc.*, 175 Cal. App. 4th 561, 568 (2009) (quoting 142 Cong. Rec. H1130 (Jan. 31, 1996)) (emphasis added). Courts have therefore held that Section 230 immunizes providers from each of the claims that Claimant asserts here:

- Breach of contract: *Smith v. Trusted Universal Standards in Elec. Transactions, Inc.*, No. 09-4567, 2011 WL 900096, at *8 (D.N.J. Mar. 15, 2011) (“Plaintiff’s [] breach of contract, and defamation claims against Cisco are dismissed” based on Microsoft’s immunity from liability under the CDA);
- Breach of the implied covenant of good faith and fair dealing: *Federal Agency of News LLC v. Facebook, Inc.*, 432 F. Supp. 3d 1107, 1120 (Section 230 immunizes Facebook from Plaintiff’s breach of the implied covenant of good faith and fair dealing claim);
- Negligence: *Riggs v. Myspace, Inc.*, 2011 WL 3020543, at *1 (9th Cir. July 25, 2011)

(plaintiff's negligence and gross negligence claims were precluded by § 230(c)(1));

- Breach of privacy: *Poole v. Tumblr, Inc.*, 404 F. Supp. 3d 637, 643 (D. Conn. 2019) (claim for invasion of privacy precluded by § 230(c)); and
- Conversion claims: *Franklin v. X Gear 101, LLC*, 2018 WL 4103492, at *8 (S.D.N.Y. Aug. 28, 2018) (conversion claim barred by § 230(c)).

Importantly, Section 230 is not “a mere defense to liability.” *Vimeo*, 991 F.3d at 73 (quoting *Nemet Chevrolet, Ltd. V. Consumeraffairs.com, Inc.*, 591 F.3d 250, 254 (4th Cir. 2009) (internal quotations omitted). Rather, it “bars lawsuit[s].” *Green v. America Online (AOL)*, 318 F. 3d 465, 471 (3d Cir. 2003); *Obado v. Magedson*, 612 Fed. App'x. 90, 93-94 (3d Cir. 2015) (plaintiff's “allegation that the defendants manipulated search engines to maximize search results relating to the alleged defamatory content does not affect their immunity from suit”) (citing *Green*, 318 F. 3d at 471); *see also Vimeo*, 991 F.3d at 73. As a result, courts “aim to resolve the question of § 230 immunity at the earliest possible stage of the case.” *Consumeraffairs.com*, 591 F.3d at 255 (citation omitted). By doing so, courts fulfill the statute's objective of avoiding providers “having to fight costly and protracted legal battles.” *Id.*

b. Microsoft Developed Standardized Protocols to Detect and Confirm CSEAI and Enforce Its Code of Conduct.

To further its commitment to creating a safe online environment, Microsoft established a Code of Conduct in the MSA that users such as Claimant must accept to use Microsoft's services. Relevant here, in agreeing to the MSA, users must not “engage in any activity that exploits, harms, or threatens to harm children,” or “engage in activity that violates the privacy of others.” MSA, ¶ 3.a.ii & 3.a.ix (Code of Conduct). The enforcement provision of the Code of Conduct states: “[i]f you violate these Terms, we may stop providing Services to you or we may close your Microsoft account.” *Id.* at ¶ 3.b.

Microsoft enforces its Code of Conduct through specialized, standardized protocols to detect, confirm, and block accounts containing CSEAI. In collaboration with Dartmouth College, Microsoft developed PhotoDNA. *See* Third Amended Demand, p. 6, ¶ 3 (citing Affidavit of Sean Davis), ¶ 4 (as modified per Microsoft's Supplemental Answer)²; Microsoft's Answer to Third Amended Demand (“Answer”) ¶ 4. PhotoDNA is an industry-leading image-matching technology that identifies and removes child sexual abuse imagery. Davis Aff. ¶ 4; Answer ¶ 4. It uses a

² For ease of review, Microsoft cites the Davis Affidavit directly throughout this motion, as “Davis Aff.” This is the same Davis Affidavit attached as Exhibit C to the Nahabet Declaration.

mathematical algorithm to create a unique signature—similar to a fingerprint—for each digital image. Davis Aff. at ¶ 5. It does this by adjusting the image to a standard size for processing, converting the image into black and white, and breaking the image into sections; calculating a unique number to represent each section; and then placing all those numbers together to create a single code that uniquely represents that image. *Id.* That code is a unique signature for the digital image, which can be compared with the signatures of other images to find copies of the original image. *Id.* This technique is known as “hashing,” *id.* at ¶ 6, and it is exceptionally accurate. PhotoDNA has an expected error rate of 1 in 50 billion. Nahabet Decl., Exhibit D, Testimony of Hany Farid, Ph.D., House Committee on Energy and Commerce, *Fostering a Healthier Internet to Protect Consumers* (“Farid Testimony”).³

PhotoDNA runs across a number of Microsoft services, including, as relevant here, in OneDrive. Davis Aff. ¶ 8. Microsoft informs users such as Claimant that it uses automated scanning technologies, including on content in OneDrive, to ensure the safety of its services. Microsoft explains this in its Privacy Statement, which is incorporated into the MSA in the first paragraph of the MSA: “1. **Your Privacy.** Your privacy is important to us. Please read the Microsoft Privacy Statement (<http://go.microsoft.com/fwlink/?LinkID=521839>) (the “**Privacy Statement**”) as it describes how Microsoft uses your content.” MSA ¶ 1.

The Privacy Statement, in turn, explains “How we use personal data.” Privacy Statement at p.6. One such use is for “**Safety**,” and there, Microsoft informs users that “some of our products, such as Outlook or OneDrive, systematically scan content in an automated manner to identify ... abusive actions....” *Id.* at p. 8. The Privacy Statement also informs users “we will retain, access, ... personal data, including your content (such as the content of your ... files in private folders on OneDrive), when we have a good faith belief that doing so is necessary to ... enforce[e] the terms governing the use of the services”). *Id.* at pp. 9-10; *see also* MSA, ¶ 3.b (Code of Conduct, Enforcement) (“When investigating alleged violations of these Terms, Microsoft reserves the right to review Your Content....”). The Privacy Statement and MSA each define “content” as including private files. *See* Privacy Statement at p. 6 (defining “**Content**” as “Content of your files and communications you input, upload, receive, create, and control”); MSA ¶ 1 (Your Privacy) (defining “**Your Content**” as “the files, photos, documents ... that you upload, store, ... through the Services”). Taken together, these provisions show Microsoft reserves the

³ Microsoft requests that the Arbitrator take judicial notice of the testimony of Hany Farid, Ph.D. before the House Committee on Energy and Commerce pursuant to New Jersey Rule of Evidence 201(b)(3).

right to scan and review private and non-private content in OneDrive.

Although PhotoDNA is exceptionally accurate, Microsoft takes seriously the ramifications of a PhotoDNA hit, Microsoft confirms through human review that all flagged images are CSEAI. Davis Aff. ¶ 10; Answer ¶ 5. If there is any question whether an image should be classified as CSEAI or not, Microsoft's human reviewers do not mark it as such. Davis Aff. ¶ 10. Microsoft's human reviewers also classify images they confirm to be CSEAI according to the age and type of act. For instance, an image classified as CSEAI A1, as is the case here, is of a sex act involving a pre-pubescent child. *Id.* at ¶ 12; Answer ¶ 7.

Once Microsoft has confirmed that an image is CSEAI, Microsoft blocks the user's access to OneDrive and suspends the account, consistent with Microsoft's Code of Conduct. MSA, ¶¶ 3.a.; 3.b. In addition, and as required by federal law, Microsoft sends a report to NCMEC. *See* 18 U.S.C. § 2258A(a).

Microsoft's actions, including scanning a user's data and suspending an account confirmed as containing CSEAI, are authorized by and consistent with the plain terms of the MSA and its Privacy Statement. Indeed, these are the steps by which Microsoft enforces the MSA's Code of Conduct.

c. PhotoDNA Detected Material Confirmed by Human Review to be CSEAI in Claimant's OneDrive.

On May 12, 2020, Microsoft's PhotoDNA technology detected and flagged as CSEAI an image in the OneDrive for the Microsoft account tomdeutsch@aol.com. Davis Aff. ¶ 12; Answer ¶ 7. The image had been independently confirmed by human review to be CSEAI and was classified as A1—a sex act involving a pre-pubescent child. Davis Aff. ¶ 12; Answer ¶ 7. Because maintaining CSEAI in OneDrive is a violation of the Code of Conduct, and because Microsoft detected and confirmed CSEAI was present in Claimant's OneDrive account, Microsoft permanently suspended his account under the MSA. Davis Aff. ¶ 13. In addition, and as required by federal law, on May 12, 2020, Microsoft filed CyberTipline report No. 72159146 with NCMEC to report the image match. *Id.* at ¶ 14; 18 U.S.C. § 2258A.

III. LEGAL STANDARD

“The sufficiency of a complaint to state a viable claim may be tested by a motion for the failure to state a claim upon which relief can be granted, and also by a motion for judgment on the pleadings.” 61 Am. Jur. 2d Pleadings § 483. “[B]oth motions can serve this purpose, and ... the

test for granting the motion is the same in either case....” *Id.* A motion for judgment on the pleadings can be made after a party has answered the complaint. *See* Pressler, Comment 4.1.1 to Rule 4:6-2 (“There is no required litany in raising the R. 4:6-2(e) defense. Thus defendant’s statement in his answer that he reserves the right to dismiss the Complaint on the ground that plaintiffs have no legal cause of action against the defendant will meet the pleading requirement of the rule.”) (citing *O’Connor v. Altus*, 67 N.J. 106, 116 (1975)). *See also* *Rapport v. Flitcroft*, 90 N.J. Super. Ct. 578, 581 (App. Div. 1966) (holding that defendant could file such motion after the answer had been filed and some discovery conducted, reasoning “it is entirely clear that this defense is not lost by failure to include it in the answer or to raise it by motion before filing an answer. It may be raised by motion for judgment on the pleadings”).

“[A] court must dismiss the plaintiff’s complaint if it has failed to articulate a legal basis entitling plaintiff to relief.” *Sickles v. Cabot Corp.*, 379 N.J. Super. 100, 105-06, (App. Div. 2005) (citing *Camden County Energy Recovery Assocs., L.P. v. New Jersey Dep’t of Env’tl. Prot.*, 320 N.J. Super. 59, 64 (App. Div. 1999) (“[N]o matter how ‘generously’ or ‘indulgently’ respondents’ pleadings are scrutinized, the conclusion is inescapable that at bottom they are no more than a fundamental challenge to decisions...for which the [defendant] should not be held judicially accountable to litigants.”)). A motion for judgment on the pleadings “under Rule 4:6-2(e) for failure to state a claim upon which relief can be granted must be evaluated in light of the legal sufficiency of the facts alleged in the complaint.” *Sickles*, 379 N.J. Super. at 106 (citation omitted).

“When considering whether a party has asserted a claim for which relief may be granted...[t]he inquiry may...include consideration of ‘exhibits attached to the complaint, matters of public record, and documents that form the basis of a claim.’” *Norcross v. Murphy*, 2020 WL 3634750, at *6 (N.J. App. Div. July 6, 2020) (citing *Banco Popular N. Am. V. Gandi*, 184 N.J. 161, 183 (2005)). Further, the “court may consider documents specifically referenced in the complaint ‘without converting the motion into one for summary judgment.’” *Id.* (quoting *Myska v. N.J. Mfrs. Ins. Co.*, 440 N.J. Super. 458, 482 (App. Div. 2015)). Although plaintiffs are generally entitled to every reasonable inference of fact, “they may not rely on conclusory allegations, hoping that discovery will allow them to find that a cause of action exists.” *Id.* (citing *Printing Mart-Morristown v. Sharp Elecs. Corp.*, 116 N.J. 739, 768 (1989) (“A plaintiff can bolster a ... cause of action through discovery, but not [] file a conclusory complaint to find out if one exists.”) (internal quotations and citations omitted)).

The MSA, including the Code of Conduct and expressly incorporated Privacy Statement, forms the basis of Claimant’s breach of contract, breach of implied covenant of good faith and fair

dealing, negligence, and breach of privacy claims. *See* Third Amended Demand at Sections II, III, IV & V. Claimant specifically references the MSA throughout his Third Amended Demand, *see, e.g.*, pp. 5, 7-8, 11, 14-16, and previously attached the MSA as an exhibit to his initial Arbitration Demand, p. 21. Moreover, Claimant also references and quotes the Affidavit of Sean Davis in his Third Amended Demand, p. 6, ¶ 3. Therefore, the Arbitrator may properly consider these documents on Microsoft's motion for judgment on the pleadings.

Because Section 230 grants immunity against suit, courts routinely address and dismiss lawsuits on Section 230 grounds at the motion to dismiss or motion for judgment on the pleadings stage. *Smith*, 2011 WL 900096 at *8 (dismissing breach of contract claims); *Facebook, Inc.*, 432 F. Supp. 3d at 1120 (dismissing breach of the implied covenant of good faith and fair dealing claim); *Riggs*, 2011 WL 3020543, at *1 (dismissing negligence and gross negligence claims); *Poole*, 404 F. Supp. 3d at 643 (dismissing breach of privacy claim); *Franklin*, 2018 WL 4103492, at *8 (dismissing conversion claim); *Dart v. Craigslist, Inc.* (granting motion for judgment on the pleadings and dismissing plaintiff's claims based on Craigslist's immunity under § 230(c)(1)). The Arbitrator should do so here, too.

IV. ARGUMENT

Section 230(c)(2)(A) provides, in relevant part: "No provider ... of an interactive computer service shall be held liable on account of— (A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider ... considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected." 47 U.S.C. § 230(c)(2)(A). Each of these conditions is satisfied here.

a. Microsoft is an Interactive Computer Service.

An "interactive computer service" is defined as "any information service, system or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet" 47 U.S.C. § 230(f)(2). "[I]nternet service providers, website exchange systems, online message boards, and search engines fall within this definition." *LeadClick*, 838 F.3d at 174 (supplying case citations). Microsoft qualifies as an interactive computer service provider when it provides the OneDrive service, as here, because through OneDrive, Microsoft gives users access to a computer server and allows users to upload, view, and share images and files. *See Holomaxx Techs. V. Microsoft Corp.*, 783 F. Supp. 2d 1097, 1104 (N.D. Cal. 2011) (finding Microsoft qualifies as an interactive

computer service); *Smith*, 2011 WL 900096, at *7 (same); *Nieman v. Versuslaw, Inc.*, No. 12-3104, 2012 WL 3201935, at *4 (C.D. Ill. June 13, 2012) (same).

b. Microsoft Blocked Claimant’s Access to OneDrive and Suspended His Account Upon Detecting and Confirming CSEAI in the Account.

Microsoft blocked Claimant’s access to OneDrive and suspended his account upon detecting and confirming that the account contained material that Microsoft “considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable.” 47 U.S.C. § 230(c)(2)(A). Although child sexual exploitation and abuse imagery is objectively objectionable, the inquiry under Section 230 is a subjective one, turning on what the provider “considers to be” any of these things. *Id.* In this way, Section 230(c)(2)(A) “does not require that the material actually be objectionable; rather, it affords protection for blocking material ‘that the provider or user *considers to be*’ objectionable.” *Zango, Inc. v. Kaspersky Lab, Inc.*, No. 07-00807, 2007 WL 5189857, at *4 (W.D. Wash. Aug. 28, 2007) (emphasis added) *aff’d*, 568 F.3d 1169 (9th Cir. 2009). This means it doesn’t matter whether Claimant agrees with Microsoft’s classification of the image as CSEAI. What matters is whether Microsoft *considers it to be*. It indisputably does, as the image was flagged by the exceptionally accurate PhotoDNA technology and had been confirmed by Microsoft’s human reviewers to be CSEAI classification A1, involving prepubescent children. There is no question that Microsoft has no tolerance for this content on its services—indeed, that is the point of the Code of Conduct. There, Microsoft required Claimant to agree he would not “engage in any activity that exploits, harms, or threatens to harm children,” or “engage in activity that violates the privacy of others.” MSA, ¶ 3.a.ii & 3.a.ix (Code of Conduct). Claimant does not—and cannot—allege facts showing Microsoft does not “consider” CSEAI objectionable. That is all that matters under Section 230(c)(2)(A)—and for good reason. If service providers such as Microsoft had to prove all content it blocked was *objectively* objectionable to avoid liability, the threat of litigation would prevent providers from developing the tools and processes necessary to ensure a safe online environment, subverting Congress’s purpose in enacting Section 230. Fortunately, that is not the law.

c. Microsoft Suspended Claimant’s Account in Good Faith, Upon Detecting and Confirming CSEAI in the Account.

When a court considers whether a provider acted in good faith under Section 230, “the appropriate question ... is whether [plaintiff] has ‘pled an absence of good faith.’” *Holomaxx*, 783

F. Supp. 2d at 1105. Because the statute couples “good faith” with the inherently subjective element—“considers to be”—the appropriate standard of review is subjective good faith. *See, e.g., Leavitt v. Yelp! Inc.*, 2011 WL 5079526, at *7 (N.D. Cal. Oct. 26, 2011) (Section 230(c)(2) includes a “subjective intent/good faith limitation” not present in § 230(c)(1)); *Vimeo*, 991 F.3d at 72.⁴

The Second Circuit’s recent decision in *Domen v. Vimeo* well-illustrates what “good faith” means under Section 230(c)(2)(A). 991 F.3d at 68.⁵ There, Vimeo suspended a user’s account after he uploaded videos promoting sexual orientation change efforts (“SOCE”). This violated Vimeo’s content policies, as Vimeo believed these videos were “harass[ing], incite[d] hatred, or include[d] discriminatory or defamatory speech.” *Id.* at 69-70. As a result, Vimeo suspended the user’s account. In response, the user sued Vimeo, asserting various state-law discrimination and constitutional claims. The district court granted Vimeo’s Rule 12(b)(6) motion to dismiss under Section 230(c), rejecting plaintiff’s bad faith arguments because “the videos promoted SOCE, violating Vimeo’s legitimate content policy against SOCE, and [plaintiff’s] allegations suggesting Vimeo acted in bad faith were too conclusory....” *Id.* at 70.

On appeal, the user argued Vimeo acted in bad faith because it had deleted the “entire account as opposed to deleting only those videos promoting SOCE”; “permitt[ed] other videos with titles referring to homosexuality to remain on the website”; and “discriminat[ed] against them on the basis of their religion and sexual orientation.” *Id.* at 68. The Second Circuit disagreed, holding plaintiff’s “allegations that Vimeo acted in bad faith are too conclusory to survive a motion to dismiss,” and also that plaintiff’s “bases for arguing that Vimeo acted in bad faith are not commensurate with how courts interpret bad faith in this context.” *Id.* at 72. The Court reasoned that Section 230(c)(2)(A) affords providers “significant subjective discretion.” *Id.* at 72. So, “Vimeo [wa]s statutorily entitled to consider SOCE content objectionable and may restrict access to that content as it sees fit.” *Id.* at 72. The Court also explained that Section 230 “does not require providers to use any particular form of restriction,” making the fact Vimeo blocked the

⁴ *See also, Rossi v. Motion Picture Ass’n of America, Inc.*, 391 F.3d 1000, 1004 (9th Cir. 2004) (“Congress understands th[e] distinction” between an objective reasonableness standard and a subjective good faith standard and “could have easily incorporated an objective standard of reasonableness”); *Sorensen v. Wolfson*, 170 F. Supp. 3d 622, 633 (S.D.N.Y. 2016) (observing that under a subjective bad faith standard, merely taking “unjustified positions” is not enough) (collecting cases); Third Amended Demand at 11 (“By their very definitions, terms like ‘inappropriate’ and ‘objectionable’ ... are subjective, not objective, standards.”).

⁵ For the Arbitrator’s convenience, Microsoft attaches as Appendix A to this Motion a copy of the *Domen v. Vimeo, Inc.* opinion.

user’s entire account—and not just the SOCE videos—“a straightforward consequence of Vimeo’s content policies” and perfectly lawful. *Id.* Nor did it matter that “other videos relating to homosexuality exist on Vimeo’s website.” *Id.* at 73. “Given the massive amount of user-generated content available on interactive platforms, imperfect exercise of content-policing discretion does not, without more, suggest that enforcement of content policies was not done in good faith.” *Id.* The Second Circuit therefore affirmed the district court’s order granting Vimeo’s motion to dismiss under Section 230(c).

So too, here. As in *Domen v. Vimeo*, Microsoft suspended Claimant’s OneDrive account in good faith, and it did so consistent with the MSA’s Privacy Statement and Code of Conduct. Microsoft suspended Claimant’s account upon detecting and confirming, through standardized processes, that the account had CSEAI in it—in violation of the explicit terms of MSA’s Code of Conduct. Claimant has not alleged, nor can he, that Microsoft did not subjectively operate in good faith. The MSA’s Code of Conduct clearly prohibits users from using Microsoft services to store child sexual exploitation and abuse imagery (just like Vimeo’s policy prohibited users from posting SOCE videos on its platform), and the Code of Conduct allows Microsoft to suspend the entirety of the OneDrive account (without returning the data) for violations (as did Vimeo’s policy). And the MSA’s Privacy Statement and Code of Conduct nowhere state Microsoft cannot or will not scan content saved to private OneDrive folders.

Quite the opposite. The MSA’s Privacy Statement expressly disclosed that “some of our products, such as ... OneDrive, *systematically scan content* in an automated manner to identify ... abusive actions,” and defined “**Content**” as the “Content of your files and communications you input, upload, receive, create, and control.” Privacy Statement, pp. 6, 8; *see also id.* at pp. 9-10 (stating Microsoft retains the right to “access ... your content (such as ... files in *private folders on OneDrive*), when we have a good faith belief that doing so is necessary to ... enforce the terms governing the use of the services”—i.e., the Code of Conduct in the MSA); MSA ¶ 1 (Privacy Statement) (defining “**Your Content**” as including “the files, photos, documents ... you upload, store ... through the Services”; ¶ 3.b. (Code of Conduct, Enforcement) reserving Microsoft’s right “to review Your Content” to enforce the Code of Conduct). Microsoft acted in accordance with the MSA’s Privacy Statement and Code of Conduct by doing what it did here—scanning a user’s content in OneDrive to identify abuses and suspend an account upon confirming a violation of the Code of Conduct. *See also USA v. Bohannon*, -- F. Supp. 3d --, 2020 WL 7319430, at *3 (N.D. Cal. Dec. 11, 2020) (defendant “consented to Microsoft’s [automated] search [of his cloud storage account] by agreeing to Microsoft’s terms of service”).

Also like the plaintiff in *Domen*, Claimant here does not—and cannot—allege that Microsoft enforced the Code of Conduct in a discriminatory fashion. Microsoft applies the MSA uniformly when, as here, PhotoDNA and human review confirm an image in a OneDrive account to be CSEAI classified as A1. Whenever this occurs, Microsoft suspends the customer’s OneDrive account, consistent with the MSA’s Code of Conduct, MSA, ¶ 3.a. & 3.b., and submits a report to NCMEC, as required by federal law, 18 U.S.C. § 2258A. There is no dispute that’s exactly what Microsoft did here.

Claimant, however, speculates that PhotoDNA got it wrong. He baselessly asserts that PhotoDNA operates like an antivirus software (it doesn’t) and the process is prone to errors (it’s not). Third Amended Demand at 5-6. And without going so far as to allege that PhotoDNA flagged the wrong account *here*, he claims “PhotoDNA can make a mistake with whose account the image is contained in.” *Id.* at 6. But while Claimant’s speculation is wholly untrue, the hypothetical possibility that PhotoDNA might have made a mistake here does not matter for purposes of Section 230(c)(2)(A). “Under the law, a mistaken choice to block, if made in good faith, cannot be the basis for liability under federal or state law.” *e360Insight, LLC v. Comcast Corp.*, 546 F. Supp. 2d 605, 609 (N.D. Ill. 2008). This is so because “[t]o force a provider ... to litigate the question of whether what it blocked was or was not [objectionable] would render § 230(c)(2) nearly meaningless.” Thus, a provider does not need to “mandate perfect enforcement of a platform’s content policies.” *Vimeo*, 991 F.3d at 68.

Nor can Claimant allege any facts even remotely similar to those courts have found constitute bad faith. For instance, because Microsoft relied on an industry-leading technology to detect the CSEAI and a human confirmation process, Claimant cannot show Microsoft failed to adhere to industry standards. *See Holomaxx Techs. v. Yahoo!, Inc.*, 2011 WL 3740827, at *2 (N.D. Cal. Aug. 23, 2011) (disregarding bad faith allegation where plaintiff failed to identify an industry standard that Yahoo! allegedly failed to follow and holding that Yahoo!’s blocking of spam was a covered action).⁶ In addition, Claimant cannot claim Microsoft has a history of targeting him or other consumers like him for anti-competitive reasons. *See e-Ventures Worldwide, LLC v. Google, Inc.*, 188 F. Supp. 3d 1265, 1271 (M.D. Fl. 2016) (declining to dismiss

⁶ See <https://blogs.microsoft.com/on-the-issues/2012/03/19/microsoft-photodna-technology-to-help-law-enforcement-fight-child-pornography/> (“NCMEC and online service providers such as Microsoft and Facebook currently use PhotoDNA to help find, report and eliminate some of the worst known images of child pornography online, helping identify thousands of these horrific images that would previously have gone undetected.”). Microsoft requests that the Arbitrator take judicial notice of this article pursuant to New Jersey Rule of Evidence 201(b)(3).

where plaintiff sufficiently alleged Google had “failed to act in good faith” where it alleged “Google has a history of targeting website owners ... and removing them from Google’s search results”). And Claimant certainly cannot show that Microsoft suspended his account for any reason other than the fact Microsoft believed the account contained content Microsoft “considers to be” objectionable (i.e., CSEAI). *See Song fi Inc. v. Google, Inc.*, 108 F. Supp. 3d 876, 883, 884 n. 3 (N.D. Cal. 2015) (removing content to artificially inflate view counts for the video content may evidence bad faith).

Claimant argues Microsoft is “seeking to streamline [its] administrative expenses through bad faith construction of [its] *resolution* policies,” apparently referring to Microsoft’s arbitration agreement. Third Amended Demand at 10 (emphasis added). But that is not an allegation that Microsoft acted in bad faith when it enforced the MSA’s Code of Conduct by suspending his account upon detecting confirmed CSEAI in his OneDrive. And to the extent Claimant complains Microsoft did not disclose the reason it had suspended his account until he filed this arbitration, that too, fails. Microsoft does not reveal to the customer that his account was closed due to a CSEAI detection unless and until the customer pursues litigation because, among other things, Microsoft cannot be complicit in the obstruction of justice. *Davis Aff.* ¶ 15. Thus, Microsoft’s refusal to tell Claimant it had found CSEAI in his account until he filed this arbitration does not evince bad faith, especially given the nature of the content at issue and the fact that Microsoft had no duty to disclose the nature of the violation. *See Holomaxx*, 783 F. Supp. 2d at 1106 (imposing “duty [on Microsoft] to discuss in detail its reasons for blocking Holomaxx’s communications or to provide a remedy for such blocking ... would be inconsistent with the intent of Congress to ‘remove disincentives for the development and utilization of blocking and filtering technologies’”) (quoting 47 U.S.C. § 230(b)(4)).

As the Second Circuit’s recent decision in *Domen v. Vimeo* shows, Section 230(c)(2)(A) grants immunity from suit for precisely the conduct at issue here: for blocking access to content that Microsoft considers to be objectionable and prohibits in its Code of Conduct, and for taking that blocking action consistent with its Code of Conduct. This makes Microsoft immune from Claimant’s causes of action, and indeed from any liability to Claimant, based on its decision to suspend Claimant’s OneDrive account upon detecting confirmed CSEAI in the account.

V. CONCLUSION

For the foregoing reasons, Microsoft respectfully requests that the Arbitrator dismiss Claimant’s Third Amended Demand with prejudice under Section 230(c)(2)(A).

Dated: May 17, 2021

RESPONDENT MICROSOFT CORPORATION

By: /s/ Natalie Nahabet

Marc R. Shapiro (NY SBN 4403606)

Natalie Nahabet (CA SBN 301597)

ORRICK, HERRINGTON & SUTCLIFFE LLP

777 South Figueroa Street, Suite 3200

Los Angeles, CA 90017

Telephone: (213) 629-2020

Facsimile: (213) 612-2499

Email: mrshapiro@orrick.com
nnahabet@orrick.com

ATTORNEYS FOR RESPONDENT MICROSOFT
CORPORATION

EXHIBIT 18

House Committee on Energy and Commerce

Fostering a Healthier Internet to Protect Consumers

Hany Farid, Ph.D.

Testimony

Background

Technology and the internet have had a remarkable impact on our lives and society. Many educational, entertaining, and inspiring things have emerged from the past two decades in innovation. At the same time, many horrific things have emerged: a massive proliferation of child sexual abuse material [5], the spread and radicalization of domestic and international terrorists [2], the distribution of illegal and deadly drugs [10], the proliferation of mis- and dis-information campaigns designed to sow civil unrest, incite violence, and disrupt democratic elections [1], the proliferation of dangerous, hateful, and deadly conspiracy theories [9], the routine harassment of women and under-represented groups in the form of threats of sexual violence and revenge and non-consensual pornography [3], small- to large-scale fraud [12], and spectacular failures to protect our personal and sensitive data [4].

How, in 20 short years, did we go from the promise of the internet to democratize access to knowledge and make the world more understanding and enlightened, to this litany of daily horrors? Due to a combination of naivete, ideology, willful ignorance, and a mentality of growth at all costs, the titans of tech have simply failed to install proper safeguards on their services.

The Past

The landmark case of *New York v. Ferber* made it illegal to create, distribute, or possess child sexual abuse material (CSAM). The result of this ruling, along with significant law enforcement efforts, was effective, and by the mid-1990s, CSAM was, according to the National Center for Missing and Exploited Children on the way to becoming a “solved problem.” By the early 2000s, however, the rise of the internet brought with it an explosion in the global distribution of CSAM. Alarmed by this growth, in 2003, Attorney General Ashcroft convened executives from the top technology firms to ask them to propose a solution to eliminate this harmful content from their networks. Between 2003 and 2008 these technology companies did nothing to address the ever-growing problem of their online services being used to distribute a staggering amount of CSAM with increasingly violent acts on increasingly younger children (as young, in some cases, as a only a few months old).

In 2008, Microsoft invited me to attend a yearly meeting of a dozen or so technology companies to provide insight into why, after five years, there was no solution to the growing and troubling spread of CSAM online. Convinced that a solution was possible, I began a collaboration with Microsoft researchers to develop technology that could quickly and reliably identify and remove CSAM from online services. Within a year we had developed and deployed such a technology –

photoDNA, a robust hashing technology¹. PhotoDNA has, in the intervening decade, seen global adoption (it is licensed at no cost) and has proven to be effective in disrupting the global distribution of previously identified CSAM: more than 95% of the nearly 18 million reports in 2018 to NCMEC's CyberTipline, constituting over 45 million pieces of identified CSAM, were from photoDNA.

This story illustrates an important point. The issue of inaction for more than five years was never one of technological limitations, it was simply an issue of will – the major technology companies at the time simply did not want to solve the problem. This is particularly inexcusable given that we were addressing some of the most unambiguously violent, heinous, and illegal content being shared on their services. The issue was, in my opinion, one of a fear. Fear that if it could be shown that CSAM could be efficiently and effectively removed, then the technology sector would have no defense for not contending with myriad abuses on their services.

The Present

In the intervening decade following the development and deployment of photoDNA, the titans of tech have barely done anything to improve or expand this technology. This is particularly stunning for an industry that prides itself on bold and rapid innovation.

In the defense of the technology sector, they are contending with an unprecedented amount of data: some 500 hours of video uploaded to YouTube every minute, some one billion daily uploads to Facebook, and some 500 million tweets per day. On the other hand, these same companies have had over a decade to get their house in order and have simply failed to do so. At the same time, they have managed to profit handsomely by harnessing the scale and volume of data uploaded to their services. And, these services don't seem to have trouble dealing with unwanted material on their services when it serves their interests. They routinely and quite effectively remove copyright infringement material (because of the Digital Millennium Copyright Act, DMCA) and adult pornography (which is a violation of, for example, Facebook's and YouTube's terms of service).

During his 2018 Congressional testimony, Mr. Zuckerberg repeatedly invoked artificial intelligence (AI) as the savior for content moderation (in 5 to 10 years time). Putting aside that it is not clear what we should do in the intervening decade, this claim is almost certainly overly optimistic.

Earlier this year, for example, Mike Schroepfer, Facebook's chief technology officer, showcased Facebook's latest AI technology for discriminating images of broccoli from images of marijuana [7]. Despite all of the latest advances in AI and pattern recognition, this system is only able to perform this task with an average accuracy of 91%. This means that approximately 1 in 10 times, the system is wrong. At the scale of a billion uploads a day, this technology cannot possibly automatically moderate content. And, this discrimination task is surely much easier than the task of identifying the broad class of CSAM, extremism, or dis-information material.

By comparison, the robust image hashing technique used by photoDNA has an expected error rate of approximately 1 in 50 billion. The promise of AI is just that, a promise, and we cannot wait a decade (or more) with the hope that AI will improve by nine orders of magnitude when it might be able to contend with automatic online content moderation.

In the meantime, AI and similar technologies can be used as a triage, reducing the amount of content that will eventually have to be viewed by human moderators. This, however, still poses considerable challenges given the woeful low number of moderators and the truly horrific working conditions that moderators are forced to endure [8].

¹Robust image hashing algorithms like photoDNA work by extracting a distinct digital signature from known harmful or illegal content and comparing these signatures against content at the point of upload. Flagged content can then be instantaneously removed and reported.

The simple fact is that the titans of tech have not invested in the infrastructure, technology, or human moderation to deal with the abuses that they know occur every day on their services. The largest point of tension is that the majority of social media is driven by advertising dollars which in turn means that they are motivated to maximize the amount of time that users spend on their services. Optimizing for the number of users and user engagement is, in many cases, at odds with effective content moderation.

End-to-End Encryption

Earlier this year, Mr. Zuckerberg announced that Facebook is implementing end-to-end encryption on its services, preventing anyone — including Facebook — from seeing the contents of any communications [14]. In announcing the decision, Mr. Zuckerberg conceded that it came at a cost:

“At the same time, there are real safety concerns to address before we can implement end-to-end encryption across all of our messaging services,” he wrote. “Encryption is a powerful tool for privacy, but that includes the privacy of people doing bad things. When billions of people use a service to connect, some of them are going to misuse it for truly terrible things like child exploitation, terrorism, and extortion.”

The adoption of end-to-end encryption would significantly hamper the efficacy of programs like photoDNA. This is particularly troubling given that the majority of the millions of yearly reports to NCMEC’s CyberTipline originate on Facebook’s Messaging services. Blindly implementing end-to-end encryption will significantly increase the risk and harm to children around the world, not to mention the inability to contend with other illegal and dangerous activities on Facebook’s services.

Many in law enforcement have made the case that a move to end-to-end encryption, without allowing access under a lawful warrant, would severely hamper law enforcement and national security efforts [13]. Programs like photoDNA, for example, would be rendered completely ineffective within an end-to-end encrypted system. In response, Attorney General Barr and his British and Australian counterparts have openly urged Mr. Zuckerberg to delay the implementation of end-to-end encryption until proper safeguards can be put in place [6], as have the 28 European Union Member States².

We should continue to have the debate between balancing privacy afforded by end-to-end encryption and the cost to our safety. In the meantime, recent advances in encryption and robust hashing technology mean that technologies like photoDNA – robust image hashing – can be adapted to operate within an end-to-end encryption system.

Specifically, when using certain types of encryption algorithms (so-called partially- or fully-homomorphic encryption), it is possible to perform the same type of robust image hashing on encrypted data [11]. This means that encrypted images can be analyzed to determine if they are known illicit or harmful material without the need, or even ability, to decrypt the image. For all other images, this analysis provides no information about its contents, thus preserving content privacy.

²The 28 EU Member States recently approved by unanimity a declaration on combating the sexual abuse of children and directly addresses this issue of end-to-end encryption writing: “Offenders make use of encryption and other anonymisation techniques to hide their identity and location. They use communication platforms hosted and administered in different countries to groom children into abuse and to extort them to obtain abusive material, as law enforcement, hampered by obfuscation techniques and different legislative regimes across different jurisdictions, especially in third countries, struggles to take forward investigations. The Council urges the industry to ensure lawful access for law enforcement and other competent authorities to digital evidence, including when encrypted or hosted on IT servers located abroad, without prohibiting or weakening encryption and in full respect of privacy and fair trial guarantees consistent with applicable law.”

Alternatively, robust image hashing can be implemented at the point of transmission, as opposed to the current approach where it is implemented upon receipt. In this client-side implementation, the distinct signature is extracted prior to encryption and transmitted alongside the encrypted message. Because no identifying information can be extracted from this signature, it does not reveal any details about the encrypted image while allowing for the monitoring of known CSAM and other harmful material.

Counter-Arguments

The argument against better content moderation and end-to-end encryption usually fall into one of several categories.

- *Freedom of expression.* It is argued that content moderation is a violation of the freedom of expression. It is not. Online services routinely ban protected speech for a variety of reasons, and can do so under their terms of service. Facebook and YouTube, for example, do not allow (legal) adult pornography on their services and do a fairly good job of removing this content. The reason they do this is because without this rule, their services would be littered with pornography, scaring away advertisers. You cannot ban protected speech and then hide behind freedom of expression as an excuse for inaction.
- *Marketplace of ideas.* It is argued that we should allow all forms of speech and then allow users to choose from the marketplace of ideas. There is, however, no counter-speech to child sexual abuse material, bomb-making and beheading videos, threats of rape, revenge porn, or fraud. And even if there was, the marketplace of ideas only works if the marketplace is fair. It is not: the online services have their thumbs on the scale because they promote content that engages users to stay on their services longer and this content tends to be the most outrageous, salacious, and controversial.
- *Sunshine.* It is argued that “sunshine is the best disinfectant,” and that the best way to counter hate-speech is with more speech. This, again, assumes a fair marketplace where ideas are given equal airtime, and that the dialogue around competing viewpoints is reasoned, thoughtful, and respectful. Perhaps this is true at the Oxford debate club, but it is certainly not the case on YouTube, Twitter, and Facebook where some of the most hateful, illegal, and dangerous content is routinely shared and celebrated. Perhaps sunshine is the best disinfectant – but for germs, not the plague.
- *Complexity.* It is argued by the technology companies that content moderation is too complex because material often falls into a gray area where it is difficult to determine its appropriateness. While it is certainly true that some material can be difficult to classify, it is also true that large amounts of material are unambiguously illegal or violations of terms of service. There is no need to be crippled by indecision when it comes to this clear-cut content.
- *Slippery slope.* It is argued that if we remove one type of material, then we will remove another, and another, and another, thus slowly eroding the global exchange of ideas. It is difficult to take this argument seriously because in the physical world we place constraints on speech without the predicted dire consequences. Why should the online world be any different when it comes to removing illegal and dangerous content?
- *Privacy.* It is argued that end-to-end encryption, without safeguards or access under a lawful warrant, is necessary to protect our privacy. Erica Portnoy, from the Electronic Frontier

Foundation (EFF), for example, argues that “*A secure messenger should provide the same amount of privacy as you have in your living room. And the D.O.J. is saying it would be worth putting a camera in every living room to catch a few child predators.*” [13] On the first part, we agree: you have certain expectations of privacy in your living room, but not absolute privacy. On the second part, we disagree: First, the DOJ is not asking to place a camera in every living room. It is asking to be allowed to view content when a lawful warrant has been issued, as it can in your living room. And lastly, is the EFF really comfortable referring to 45 million pieces of child sexual abuse material reported to NCMEC last year as “a few child predators?”

Conclusions

We can and we must do better when it comes to contending with some of the most violent, harmful, dangerous, and hateful content online. I reject the naysayers that argue that it is too difficult or impossible, or those that say that reasonable and responsible content moderation will lead to the stifling of an open exchange of ideas.

References

- [1] S. Bradshaw and P. Howard. The global disinformation order. *Computational Propaganda Research Project*, Sep 2019.
- [2] M. Fisher and A. Taub. How everyday social media users become real-world extremists. *New York Times*, Apr 2018.
- [3] S. Haynes. ‘A toxic place for women.’ a new study reveals the scale of abuse on Twitter. *Time*, Dec 2018.
- [4] V. Ho. Facebook’s privacy problems: a roundup. *The Guardian*, Dec 2018.
- [5] M. Keller and G. Dance. The internet is overrun with images of child sexual abuse. what went wrong? *New York Times*, Sep 2019.
- [6] R. McMillan, J. Horwitz, and D. Volz. Barr presses Facebook on encryption, setting up clash over privacy. *Wall Street Journal*, Oct 2019.
- [7] C. Metz and M. Isaac. Facebook’s A.I. whiz now faces the task of cleaning it up. sometimes that brings him to tears. *New York Times*, May 2019.
- [8] C. Newton. Bodies in seats. *The Verge*, Jun 2019.
- [9] B. Resnick. Social media’s conspiracy theory problem isn’t going away. *Vox*, Aug 2019.
- [10] D. Scott. This is how easy it is to order deadly opioids over the internet. *Vox*, Jan 2018.
- [11] P. Singh and H. Farid. Robust homomorphic image hashing. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops*, pages 11–18, 2019.
- [12] S. Tompor. Scammers are fooling millennials out of millions of dollars: Here’s how. *Detroit Free Press*, Oct 2019.
- [13] J. Valentino-DeVries and G. Dance. Facebook encryption eyed in fight against online child sex abuse. *New York Times*, Oct 2019.
- [14] M. Zuckerberg. A privacy-focused vision for social networking, Mar 2019.

EXHIBIT 19

AMERICAN ARBITRATION ASSOCIATION

THOMAS DEUTSCH, ESQ.,

Claimant,

v.

MICROSOFT CORPORATION,

Respondent.

:
:
:
:
:
:
:
:
:
:

CASE NO. 01-20-0014-3715

RESPONDENT MICROSOFT CORPORATION'S
OPPOSITION TO CLAIMANT'S MOTION TO COMPEL

Table of Contents

I. Introduction	3
II. Background	5
III. Argument.....	6
a. The Arbitrator Should Deny Claimant’s Motion Because Microsoft Is Immune from Suit Under Section 230(c)(2)(A).	6
b. The Arbitrator Should Deny Claimant’s Motion Because It Seeks to Compel Microsoft to Violate Federal Law.	9
c. The Arbitrator Should Deny Claimant’s Motion Because Alternatives Are Available.	13
IV. Conclusion	14

I. Introduction

Claimant brought this action after Microsoft blocked his access to OneDrive and suspended his account upon detecting confirmed child sexual exploitation and abuse imagery (“CSEAI”) in the account—a serious violation of Microsoft’s Code of Conduct. Microsoft has no tolerance for child sexual exploitation and abuse imagery on its services and has long committed to ensuring its services are safe and free from such illegal content, including through the use of technology and processes to detect and block CSEAI and enforce the Code of Conduct.¹ See Declaration of Natalie Nahabet (the “Nahabet Decl.”)² Exhibit A, Microsoft Services Agreement (“MSA”) ¶ 3.a. & 3.b.; Exhibit B, Privacy Statement pp. 6, 8-10. That is precisely what occurred here, when Microsoft’s industry-leading PhotoDNA hash-matching technology identified an image in Claimant’s OneDrive that Microsoft human reviewers had confirmed to be A1—a sex act involving a pre-pubescent child, the most egregious form of this imagery. Although Microsoft has offered to remove and destroy the CSEAI image from Claimant’s OneDrive and restore access to his account, Claimant rejected that because he is not satisfied. He wants more—specifically, he wants Microsoft to distribute the A1, illegal child sexual exploitation and abuse image to him, and he asks the Arbitrator to order this distribution.

The Arbitrator should deny Claimant’s motion to compel for at least three independently sufficient reasons:

First, Section 230 of the Communications Decency Act (“CDA”) grants Microsoft immunity from Claimant’s lawsuit, obviating any need for the Arbitrator to even reach Claimant’s motion to compel. As Microsoft also explains in its simultaneously filed Motion for Judgment on the Pleadings, under Section 230, Microsoft may not be held liable for “any action voluntarily taken in good faith to restrict access to ... material that the provider ... considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable....” 47 U.S.C. § 230(c)(2)(A). This immunity turns on whether Microsoft *subjectively* believed that the CSEAI it

¹ See <https://blogs.microsoft.com/on-the-issues/2020/01/09/artemis-online-grooming-detection/> (“Online child exploitation is a horrific crime that requires a whole-of-society approach. Microsoft has a long-standing commitment to child online protection. First and foremost, as a technology company, we have a responsibility to create software, devices and services that have safety features built in from the outset. We leverage technology across our services to detect, disrupt and report illegal content, including child sexual exploitation. And we innovate and invest in tools, technology and partnerships to support the global fight needed to address online child sexual exploitation.”).

² Unless specified, all citations to exhibits are to those exhibits attached to the Nahabet Declaration, submitted concurrently herewith.

detected was any one of these things, and on whether it blocked Claimant's access to OneDrive in good faith as a result. There is no question that Microsoft's Code of Conduct identifies CSEAI as among the types of content that Microsoft prohibits on its services. And, as Microsoft has shown, it has standardized and robust procedures for detecting and blocking access to CSEAI on its services. *See* Answer to Third Amended Demand ¶¶ 4-6; Nahabet Decl., Exhibit C, Davis Aff. ¶¶ 5-11. Microsoft's conduct here falls squarely within Section 230(c)(2)(A), and the Arbitrator should deny Claimant's motion to compel on this basis.

Second, even if the Arbitrator were to reach the merits of Claimant's motion, it should still deny it because compelling Microsoft to distribute CSEAI to Claimant would necessarily amount to ordering Microsoft to violate federal law. Multiple criminal statutes prohibit distribution of child pornography and sexually explicit material involving a minor. 18 U.S.C. §§ 2252, 2252A. This prohibition is categorical. Microsoft is unaware of any exception, and Claimant has identified none. In an effort to minimize the unprecedented nature of his request, Claimant cites to various New Jersey state law criminal and civil cases. But each involves a disclosure *by law enforcement*, not a private party such as Microsoft, who is subject to criminal penalties under federal law. What's more, this is not a criminal proceeding where constitutional due process rights are at stake. This is a civil, consumer arbitration involving contract and tort claims. Claimant's cases simply have no application here, and he cites no authority supporting the extraordinary relief he seeks.

Third, even if all that were otherwise (and it is not), there is no need to compel Microsoft to distribute CSEAI because Claimant can obtain the image or its functional equivalent from alternative sources, without requiring Microsoft to violate federal law. As a threshold matter, Claimant has represented to Microsoft that he has the image. That, alone, moots this motion to compel. Even if Claimant felt the need to compare the image he has in his files with the image Microsoft detected, he is free to subpoena the National Center for Missing & Exploited Children ("NCMEC") for the image, as Microsoft was required by federal law to send the image to NCMEC upon detecting it. 18 U.S.C. § 2258A. There is yet a third, even easier alternative to compelling Microsoft to violate federal law. Based on Claimant's representations, the image he believes triggered PhotoDNA here is the same image that has been litigated in another civil proceeding outside the United States. In that case, because it was proceeding in an international forum, NCMEC supplied a declaration that described the image. That description informed the court's determination that the image is illegal and its existence in that plaintiff's OneDrive (whether the plaintiff ever shared the image or not) violated Microsoft's Code of Conduct.

Microsoft attaches this NCMEC declaration as Exhibit E to the Declaration of Natalie Nahabet, filed with this opposition brief. Because an official description of the image is available for Claimant and the Arbitrator, there is simply no need for the Arbitrator to require Microsoft to distribute child sexual exploitation and abuse imagery in violation of federal law.

II. Background

On May 12, 2020, Microsoft's PhotoDNA technology detected child sexual exploitation and abuse imagery in Claimant's OneDrive account. Exhibit C, Affidavit of Sean Davis ("Davis Aff.") ¶ 12 (as modified per Microsoft's Supplement to its Answer). Microsoft's trained human reviewers had confirmed the image was CSEAI, with an A1 classification, meaning it was a sex act involving a pre-pubescent child. *Id.* This is the most serious form of this imagery. *Id.*

As required by federal law, 18 U.S.C. § 2258A, upon detecting confirmed CSEAI, Microsoft sent a CyberTipline report to NCMEC, which included the image.³ Consistent with the MSA's Code of Conduct, Microsoft blocked Claimant's access to OneDrive and suspended his account. Exhibit C, Davis Aff. ¶¶ 3, 13; Exhibit A, MSA ¶ 3a.ii. & 3a.ix.

On August 14, 2020, Claimant filed this arbitration demand seeking the data in his OneDrive account—including, apparently, the child sexual exploitation and abuse image itself. In January 2021, the Arbitrator denied Claimant's "emergency" motion for return of this data. On March 7, 2021, Claimant filed the Third Amended Arbitration Demand. Microsoft filed an answer and defenses, as well as a supplemental answer.

Now Claimant doubles down and moves the Court for an order compelling Microsoft to turn over the child sexual exploitation and abuse image despite the fact he claims to have the image in his possession. *See Nahabet Decl.* at ¶ 6. Specifically, throughout this litigation, Claimant has maintained that the image flagged by PhotoDNA displays a male adult standing on the beach with swim trunks and with two young children in the corner engaging in indecent activity. *Nahabet Decl.* at ¶ 6. Based on Claimant's description of the image, Microsoft believes

³ Claimant operates under the flawed assumption that because Microsoft reported the image to NCMEC, if he had done anything illegal he would already have been contacted by law enforcement. *Mot. to Compel* at 4. Claimant cites nothing to show law enforcement conducts criminal investigations for each of the tens of millions of CyberTipline reports it receives, or that it would have done so by now given the criminal statutes of limitations. *See, e.g.,* <https://www.missingkids.org/footer/media/keyfacts> ("In 2020 the CyberTipline received more than 21.7 million reports, most of which related to: Apparent child sexual abuse material..."). What's more, law enforcement has plenty of covert investigation mechanisms available to it, so the fact neither Claimant nor Microsoft is aware of a criminal investigation is neither here nor there.

this is the same image that NCMEC described in an official declaration in another civil proceeding. Consistent with Claimant’s own description of the image, NCMEC described the image at issue as depicting “an adult male, clothed from the waist down, seen standing on a beach, while two prepubescent children appear to be unclothed and simulating a sexual position in the background of the image.” *Id.* at Ex. E, ¶ 10. In that case, the court relied on NCMEC’s declaration, among other things, to conclude: “[e]ven if only the *suggestion* is created that the children depicted are having sexual contact, ... [the image] is a visual representation of children participating in real or simulated explicit sexual acts ... [and] is therefore child pornography....” *Id.* at Ex. F, ¶ 4.8.

III. Argument

The unprecedented and extraordinary nature of the relief Claimant requests here cannot be understated. Ruling in Claimant’s favor will mean Microsoft will be required to distribute child sexual exploitation and abuse imagery in violation of federal law, and it will be required to do so as a private party, in the context of a civil proceeding, to a civil litigant who—for all Microsoft knows—may well still be subject to criminal investigation and prosecution. There is no need for the Arbitrator to wade into this morass. Section 230(c)(2)(A) bars Claimant from suing Microsoft, federal law prohibits Microsoft from distributing the CSEAI, and Claimant has at least three alternatives available to him, each of which avoids compelling Microsoft to violate federal law. Any one of these reasons requires denying Claimant’s motion; all three exist here.

a. The Arbitrator Should Deny Claimant’s Motion Because Microsoft Is Immune from Suit Under Section 230(c)(2)(A).

As explained more fully in Microsoft’s parallel Motion for Judgment on the Pleadings under Section 230, that statute grants Microsoft immunity from the claims asserted here, supplying a threshold basis for denying Claimant’s motion. *See, e.g., Smith v. Trusted Universal Standards in Elec. Transactions, Inc.*, No. 09-4567, 2011 WL 900096, at *8 (D.N.J. Mar. 15, 2011) (“Plaintiff’s [] breach of contract, and defamation claims against Cisco are dismissed” based on immunity from liability under the CDA). To incentivize interactive computer service providers such as Microsoft to police their platforms, Congress included a “Good Samaritan” safe harbor in the CDA. That safe harbor provides:

(2) Civil Liability

No provider ... of an interactive computer service shall be held liable on account of—

(A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider ... considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable....

47 U.S.C. § 230(c)(2)(A). This turns on the service provider’s *subjective* decision that the content was one of these things—i.e., what the service provider “considers to be” any of these things. *Id.*; *Zango, Inc. v. Kaspersky Lab, Inc.*, No. 07-00807, 2007 WL 5189857, at *4 (W.D. Wash. Aug. 28, 2007) (emphasis added) *aff’d*, 568 F.3d 1169 (9th Cir. 2009). In other words, and as the Second Circuit recently made clear, Section 230 immunity does not rise or fall based on whether *others*, such as Claimant, agree with Microsoft’s subjective determination. *Domen v. Vimeo, Inc.*, 991 F.3d 66, 72 (2d Cir. 2021).

In addition, courts have confirmed that “good faith” means the provider did not act arbitrarily or in bad faith, such as with intent to target the specific plaintiff. *See, e.g., e-Ventures Worldwide, LLC v. Google, Inc.*, 188 F. Supp. 3d 1265, 1271 (M.D. Fl. 2016). As the Second Circuit explained in *Domen v. Vimeo*, Section 230(c)(2)(A) “does not require interactive service providers to use a particular method of content restriction, nor does it mandate perfect enforcement of a platform’s content policies.” 991 F.3d 66, 68 (2d Cir. 2021). Indeed, under Section 230(c)(2)(A), “a mistaken choice to block, if made in good faith, cannot be the basis for liability under federal or state law.” *e360Insight, LLC v. Comcast Corp.*, 546 F. Supp. 2d 605, 609 (N.D. Ill. 2008). So, for instance, in *Domen*, the Second Circuit held Vimeo was immune from claims based on its decision to block a user’s entire account—as opposed to only the content it deemed objectionable—when the user posted videos about sexual orientation change efforts, because those videos violated Vimeo’s terms of use. 991 F.3d at 72.

Here, there is no question Microsoft “considers” CSEAI to be “obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable.” Microsoft’s Code of Conduct in the MSA requires users, such as Claimant, to follow its “rules,” including: “Don’t engage in any activity that exploits, harms, or threatens to harm children.” Exhibit A, MSA ¶ 3.a.ii. There is no dispute that Microsoft’s PhotoDNA hash-matching technology identified the image at issue here as CSEAI, and that Microsoft human reviewers had confirmed this same image to be CSEAI, classified as A1. Exhibit C, Davis Aff. ¶ 12. These are all the facts necessary to conclude that Microsoft *subjectively* believed the image to be what it said it was: child sexual exploitation and abuse imagery—a type of content that Microsoft expressly prohibits in its Code of Conduct.

Nor is the physical image relevant to whether Microsoft acted in good faith in blocking Claimant’s access to OneDrive and suspending his account after detecting confirmed CSEAI in it.

As Microsoft explained in detail in its Opposition to Claimant’s Motion for Emergent Relief, Microsoft used standardized technology and procedures designed to identify CSEAI, and to do so with exceptional accuracy, buttressed by human confirmation. Opposition to Claimant’s Motion for Emergent Relief, II.b. & II.d. PhotoDNA uses a robust hashing technology to scan user-generated content against a database of hashes of known images of child sexual exploitation and abuse, which have been provided by NCMEC, an independent third party. Exhibit C, Davis Aff. ¶ 8. PhotoDNA identifies CSEAI with exceptional accuracy. *Id.* at ¶ 5. Dr. Hany Farid, a leading digital-imaging expert and computer scientist professor who collaborated with Microsoft in developing the PhotoDNA technology, has testified that PhotoDNA “has an expected error rate of approximately 1 in 50 billion.” Exhibit E, Testimony of Hany Farid, Ph.D., House Committee on Energy and Commerce, Fostering a Healthier Internet to Protect Consumers.

Although PhotoDNA is exceptionally accurate, Microsoft ensures that images flagged by PhotoDNA have also been confirmed to be CSEAI through human review, thereby ensuring a robust and fair process. Exhibit C, Davis Aff. ¶ 10. Through the human review part of this process, Microsoft classifies images it has confirmed to be CSEAI according to the age and type of act. *See, e.g., id.* at ¶ 12. If there is any question as to whether an image should be classified as CSEAI or not, it is not marked as such. *Id.* at ¶ 10. In the face of these specialized, standard, and robust protocols, Claimant cannot establish any arbitrary or bad faith conduct by Microsoft. That Microsoft’s PhotoDNA scanned the CSEAI even though Claimant had not taken action to “share” it with someone else makes no difference. Setting aside the fact that the MSA’s Privacy Statement and Code of Conduct allowed it to scan Claimant’s content regardless whether it was in a private or shared folder, “good faith” does not “mandate perfect enforcement of a platform’s content policies.” *Domen*, 991 F.3d at 68; Ex. A, MSA ¶ 1 (“**Your Privacy.** Your privacy is important to us. Please read the Microsoft Privacy Statement” and providing a hyperlink to the statement, thereby incorporating the Privacy Statement into the MSA); Ex. B, Privacy Statement. Put simply, immunity under Section 230(c)(2)(A) applies here, and the physical image is neither relevant nor necessary to this determination.

Claimant has no meaningful response. Instead, he argues the Arbitrator should require Microsoft to distribute child sexual exploitation and abuse imagery in violation of federal law out of “fairness and equipoise.” *Mot to Compel.* at 9. But Microsoft will be relying on its industry-leading, highly accurate PhotoDNA technology and human review process in this case—not the physical image—so “fairness and equipoise” provide no justification for the unprecedented relief Claimant seeks. This also means there is no reason for the Arbitrator to order that Microsoft is

“precluded from relying upon the image in its defense during this arbitration.” Mot. to Compel. at 9. Microsoft already has no intention of relying on the physical image in this case.

Because Section 230(c)(2)(A) applies and bars Claimant’s claims, Microsoft is immune from Claimant’s suit and the Arbitrator need never reach the merits of his demand that Microsoft distribute CSEAI to him. The Arbitrator should deny Claimant’s motion to compel on this basis, alone.

b. The Arbitrator Should Deny Claimant’s Motion Because It Seeks to Compel Microsoft to Violate Federal Law.

Even if the Arbitrator were to reach the merits of Claimant’s motion (and as discussed above, the Arbitrator need not), the Arbitrator should still deny it. A contrary result here would mean the Arbitrator would be requiring Microsoft to knowingly distribute the child sexual exploitation and abuse image. That violates 18 U.S.C. §§ 2252(a)(2) and 2252A(a)(2). Claimant has identified no exception to this federal prohibition. “An arbitrator cannot order a party to perform an illegal act.” *Party Yards, Inc. v. Templeton*, 751 So. 2d 121, 123 (Fla. Dist. Ct. App. 2000) (citing *Hill v. Norfolk & W.Ry. Co.*, 814 F.2d 1192, 1195 (7th Cir. 1987) (“A party can complain if the arbitrators’ decision is infected by fraud or other corruption, or if it orders an illegal act.”)). This ground, too, requires denying Claimant’s motion.

Congress has enacted comprehensive federal child pornography laws to protect children throughout the United States from sexual exploitation and the continuing harm such material causes. *See generally* 18 U.S.C. §§ 2251, 2252, & 2252A. The very possession of such imagery is a federal and state criminal offense. 18 U.S.C. § 2252(a)(4); N.J.S.A. 2C:24-4(5)(a)(ii) and (5)(a)(iii). More egregious, the knowing receipt or distribution of child sexual exploitation and abuse imagery by any means in interstate commerce, including by computer, is unlawful. 18 U.S.C. § 2252(a)(2) (criminalizing knowing receipt or distribution through interstate commerce by any means, including by computer, the visual depiction of a minor engaging in sexually explicit conduct); *id.* at § 2252A(a)(2) (criminalizing knowing receipt or distribution of child pornography through interstate commerce, including by computer). Yet this is exactly what Claimant asks the Arbitrator to compel Microsoft to do—knowingly distribute an image that PhotoDNA flagged, that Microsoft’s human reviewers confirmed was CSEAI classification A1, and that based on Claimant’s own description of the image, has been declared illegal child sexual exploitation and abuse imagery.⁴ *See, e.g.*, Nahabet Decl at Ex. F, ¶ 4.8 (finding the image Claimant argues

⁴ If the Arbitrator requires Microsoft to distribute the CSEAI to Claimant, Microsoft would also be required, under 18 U.S.C. § 2258A, to submit a CyberTipline report to NCMEC reporting the

triggered PhotoDNA here to be illegal child pornography). This is true even if distribution is limited to “the Arbitrator herself, counsel [for the parties], and for an independent review by a third party to issue an expert opinion,” Mot. to Compel at 8, as federal law provides *no* exception to the categorical bar on distributing CSEAI.

Precisely because child pornography is illegal contraband, courts have categorically prohibited the reproduction of this harmful material even in criminal proceedings. *See, e.g., United States v. Horn*, 187 F.3d 781, 792 (8th Cir. 1999) (holding trial court was authorized under Rule 16 to deny defendant’s motion seeking to obtain copies of video tapes containing child pornography that were going to be used against him at trial); *United States v. Kimbrough*, 69 F.3d 723, 731 (5th Cir. 1995) (holding “[c]hild pornography is illegal contraband”; therefore, Rule 16 does not provide for the distribution or copying of the material by the defense). Congress has explicitly set forth the conditions under which a *criminal* defendant or his counsel may access such contraband, but these conditions do *not* include dissemination: “In any criminal proceeding, any property or material that constitutes child pornography...shall remain in the care, custody, and control of either the Government or the court.” 18 U.S.C. § 3509(m)(1). Indeed, Congress strictly prohibits a *criminal* defendant from “copy[ing], photograph[ing], duplicat[ing], or otherwise reproduc[ing] any property or material that constitutes child pornography...so long as the Government makes the property or material reasonably available to the defendant.” *Id.* at § 3509(m)(2)(A). “Congress did not want defense counsel to view, let alone possess, existing child pornography without governmental oversight.” *Doe v. Boland*, 630 F.3d 491, 495 (6th Cir. 2011). As this shows, even criminal defendants may not obtain the type of access and relief that Claimant requests here.

Nor has Congress prescribed any procedure by which a civil litigant may either obtain or access child sexual exploitation and abuse imagery in civil litigation. Civil parties such as Microsoft and Claimant are not subject to the same immunity applicable to “judges, grand jurors and prosecutors in carrying out their official duties.” *Id.* at 498. So, for instance, in *Doe v. Boland*, 630 F.3d 491 (6th Cir. 2011), where a criminal defendant argued he did not violate 18 U.S.C. § 2252(a)(4) because he could “not determine whether what he is viewing is an actual or virtual image of a child,” the Court held that federal law contained no exceptions for the defendant’s expert witness. There, the expert had taken innocuous stock photos of children and digitally altered them to create pornographic material (e.g., replacing the doughnut being eaten by

apparent violations of 18 U.S.C. §§ 2252 and 2252A by all parties involved.

a child with a penis). *Id.* The Court held that by doing so, and by retaining the resulting images, the expert had violated § 2252A(a)(5)(B) and was subject to a federal criminal investigation, causing the expert to enter a pre-trial diversion agreement with the U.S. Attorney’s office. *Id.* at 494. The expert was also subject to a civil suit by the parents of the minor children.

In holding the law provided no exception for an expert witness for a criminal defendant, the Court was unequivocal: “[N]o constitutional principle ... allows a criminal defendant to defend *one* criminal charge by urging his lawyer or witness to commit *another*.” *Id.* at 496 (emphasis in original). This rationale applies with even more force here, in a civil proceeding, where Claimant asks the Arbitrator to order Microsoft to distribute CSEAI—the very content Microsoft has committed to eliminating from its services to protect children and families—in violation of federal law.

Claimant seeks to circumvent this federal bar on distributing CSEAI by resorting to inapplicable New Jersey case law. *See* Mot. to Compel at 6-8. The Arbitrator should reject this invitation. If the Arbitrator were to order Microsoft to distribute the CSEAI here, that would necessarily trigger §§ 2252(a)(2) and 2252A(a)(2). This is so because it would result in Microsoft distributing an image it knows to be child sexual exploitation and abuse imagery through interstate commerce and across state lines: from Washington (where Microsoft is) to New Jersey (where Claimant is), New York (where Claimant’s counsel is), and Florida (where the Arbitrator may be). Claimant does not explain how New Jersey state law could possibly override this federal prohibition on knowing, interstate distribution of CSEAI, and it does not. None of Claimant’s New Jersey cases involve facts even remotely similar to this case, or any discussion of the federal laws that apply here.

Indeed, and contrary to Claimant’s assertion, New Jersey law does *not* allow for the distribution of child sexual exploitation and abuse imagery in this civil arbitration. In *State v. Scoles*, the New Jersey Supreme Court addressed the rights of a criminal defendant who, under the Sixth Amendment to the United States Constitution (and Article I of the New Jersey Constitution), was guaranteed “the unfettered access and assistance of his counsel.” 214 N.J. 236 (2013) (citing *Marshall v. Rodgers*, 569 U.S. 58, 62 (2013) (“It is beyond dispute that [t]he Sixth Amendment safeguards to an accused who faces incarceration the right to counsel at all critical stages of the criminal process.” (internal quotations omitted))). Nor did this case invoke §§ 2252 and 2252A, as there was no issue of knowing distribution across state lines. Claimant has not offered any reason, nor does he argue, that he is similarly situated to a criminal defendant facing incarceration and entitled to constitutional protections provided to such criminal defendants.

Nor does *G.A.-H v. K.G.G.*, 455 N.J. Super. 294, 299 (2018), have any application here. As a threshold matter, the plaintiff in this case was the minor *victim* of the sexual abuse who, after a criminal investigation, brought a civil action for compensation. The Appellate Division found that procedural posture—a minor victim’s suit for compensation against the perpetrator—critically relevant in determining whether the victim-plaintiff should have access to the criminal material. As the court explained, “[w]e cannot imagine the Legislature intended to frustrate a victim’s pursuit of a civil remedy by invoking the very laws designed to protect her.” *Id.* at 299. In addition, there the party compelled to disclose the CSEAI was the County Prosecutor’s office, not a private actor. Prosecutors, however, are immune from liability for acts arising from carrying out their official duties, which undoubtedly includes compliance with a court order. *Doe*, 630 F.3d at 498. In any event, the New Jersey Supreme Court *reversed* the Appellate Division holding on which Claimant relies here. *See G.A.-H. v. K.G.G.*, 238 N.J. 401, 407 (2019) (reversing and reinstating summary judgment, thereby nullifying the Appellate Division’s holding regarding scope of discovery on remand).

That federal law contains no exception for civil litigation makes good sense. Every time a child sexual exploitation and abuse image is reproduced, the harm suffered by the pre-pubescent child depicted in the image is further perpetuated. *United States v. Goff*, 501 F.3d 250, 259 (3d Cir. 2007); *see also Osborn v. Ohio*, 495 U.S. 103, 111 (1990) (“The pornography’s continued existence causes the child victims continuing harm by haunting the children in years to come.”). The “simple fact that the images have been disseminated perpetuates the abuse” captured in the image. *United States v. Norris*, 159 F.3d 926, 929 (5th Cir. 1998). Indeed, the “mere existence of the child pornography invades the privacy of the child depicted.” *United States v. Paroline*, 672 F. Supp. 2d 781, 786 (E.D. Tex. 2009), *aff’d en banc sub nom. In re Amy Unknown*, 701 F.3d 749 (2012), *vacated on other grounds*, 572 U.S. 434 (2014). Congress has recognized the profound nature of this ongoing harm. In the Effective Child Pornography Prosecution Act of 2007, Congress found that such images are “a permanent record of a child’s abuse and the distribution of child pornography images revictimizes the child.” Pub. L. 110-358, title I, § 102(3), Oct. 8, 2008, 122 Stat. 4001 (“2007 Act”); *see also* Child Pornography Prevention Act of 1996, Pub. L. 104-208, § 121, 110 Stat. 3009-26 (congressional finding that an image’s “continued existence causes the child victims of sexual abuse continuing harm by haunting those children in future years”).

What Claimant asks the Arbitrator to do here is truly astounding. Claimant not only seeks to compel a violation of federal law, but also to perpetuate the abuse depicted in the image—the

very harm Microsoft seeks to prevent from occurring on its services. No basis in law or fact supports Claimant's demand, and the Arbitrator should deny it.

c. The Arbitrator Should Deny Claimant's Motion Because Alternatives Are Available.

Even if all that were otherwise (and it is not), the Arbitrator should still deny Claimant's motion because alternatives to distribution of the physical child sexual exploitation and abuse image are available to him, obviating the need to even entertain Claimant's motion.

For one, Claimant's own description of the image shows he clearly still has it. Because he has it, no basis exists for compelling Microsoft to knowingly distribute child sexual exploitation and abuse imagery to Claimant in violation of federal law.⁵

In addition, Claimant is free to issue a subpoena to NCMEC. NCMEC manages the centralized reporting for the online exploitation of children through its CyberTipline. Under § 2258A(g)(3), "NCMEC may disclose by mail, electronic transmission, or other reasonable means, information received in a report under subsection (a) only to ... (E) respond to legal process, as necessary." Claimant is welcome to invoke this alternative—one that threatens no one with criminal penalties and that provides the very relief he seeks.

And in the meantime, Claimant now has the official NCMEC description of the image. *See* Nahabet Decl., Ex. E. That he does so makes compelled production of the physical image in violation of federal law entirely unnecessary. Indeed, a court in the Netherlands relied on NCMEC's declaration, among other things, in ruling on nearly identical claims. And there, the court held the image was illegal CSEAI and its existence in the plaintiff's OneDrive account violated Microsoft's Code of Conduct, even if the plaintiff never "shared" the image. *See id.* at Ex. F, ¶ 4.8. Just as the NCMEC description informed the Netherlands court's determination, so too the declaration's description will suffice to allow the Arbitrator to rule on Claimant's claims here.

At bottom, there is simply no justification for the unprecedented ruling Claimant asks the Arbitrator to make here, and the Arbitrator should deny Claimant's motion.

//

//

//

⁵ Microsoft would be willing to identify the file path for the image (i.e., the file name reflecting the directory tree hierarchy where the image was stored), so Claimant may further research the image.

IV. Conclusion

For these reasons, Microsoft respectfully requests that the Arbitrator deny Claimant's motion to compel.

Dated: May 17, 2021

RESPONDENT MICROSOFT CORPORATION

By: /s/ Natalie Nahabet
Marc R. Shapiro (NY SBN 4403606)
Natalie Nahabet (CA SBN 301597)
ORRICK, HERRINGTON & SUTCLIFFE LLP
777 South Figueroa Street, Suite 3200
Los Angeles, CA 90017
Telephone: (213) 629-2020
Facsimile: (213) 612-2499
Email: mrshapiro@orrick.com
nnahabet@orrick.com

ATTORNEYS FOR RESPONDENT MICROSOFT
CORPORATION

EXHIBIT 20

From: Harriet Derman <hderman@newjerseylaw.net>
Sent: Tuesday, May 18, 2021 4:19 PM
To: Nahabet, Natalie; Shapiro, Marc R.; cc: Frank Salzano; Efthimios Parasidis
Subject: unpublished opinion

Dear Ms. Nahabet,

At your convenience could you please forward by overnight mail, no rush, the unreported decisions of Smith v. Trusted Universal Stds. and Zango v. Kaspersky Lab. I just could not locate them on Lexis, which is the source my law firm uses.
Thanks. Judge Derman

EXHIBIT 21

From: Jason Lampert <jlampert@slwlawoffices.com>
Sent: Wednesday, May 26, 2021 9:08 AM
To: Harriet Derman
Cc: Nahabet, Natalie; Frank Salzano; Efthimios Parasidis; Shapiro, Marc R.; AAA Jenna Pascale
Subject: Deutsch v Microsoft - AAA 01-20-0014-3715

Dear Judge Derman,

Pursuant to AAA Consumer Arbitration Rule R-8, we write to request leave to amend the claim in this matter. The very limited discovery that has occurred has brought new, material information to light. An amendment to the claim is essential in order to conform the pleadings to update the relevant facts and related legal claims. We summarize the material facts herein:

First, through discovery Microsoft admitted that they now believe Claimant did not share any CSEAI via OneDrive or any other means at any time, contrary to Microsoft's previous Answers and Affidavit(s).

Second, through discovery Microsoft further admitted that its PhotoDNA program has been scanning the private files of OneDrive clients on a system-wide basis, including Claimant's, which is in direct violation of the MSA and Privacy Statement (which only permits scanning of files shared via OneDrive, not files simply stored on OneDrive). Moreover, Microsoft's scanning of private files is in direct contravention to all of the core rules of Microsoft's own internal policies and procedures for OneDrive scanning.

Third, we recently received Claimant's phone and text logs from Verizon (in response to our prepared subpoena that was issued to Verizon). Those phone and text logs reveal that Claimant had not used his phone for voice or text anytime near the time on May 12, 2020 when Microsoft improperly scanned his private files and reported Claimant to the NCMEC. The logs further substantiate that, even if there was some alleged CSEAI, Claimant was a passive recipient of such image and did not actively or knowingly receive the image. Given that Microsoft has failed to provide Claimant with any indication of what image actually triggered PhotoDNA, further discovery is necessary to unpack the issues in this case.

Each of these facts is material to the claim, and directly relevant to the pending motions.

For these reasons, we respectfully request leave to amend the claim. We can submit the amendment on or before June 8, 2021.

Respectfully submitted,

Jason Lampert
Salzano, Lampert & Wilson, LLP
275 Madison Avenue, 35th Floor
New York, NY 10016
Telephone: (646) 863-1883
Facsimile: (646) 365-3119

www.slwlawoffices.com

NOTICE: This message and its attachments are sent from a law office and may contain information that is confidential and protected by privilege from disclosure. If you are not the intended recipient, you are prohibited from printing, copying, forwarding or saving them. Please delete the message and attachments without printing, copying, forwarding or saving them, and notify the sender immediately.

Disclosure under IRS Circular 230: To ensure compliance with requirements imposed by the IRS, we inform you that any tax advice contained in this communication (including any attachments) was not intended or written to be used, and may not be used, for the purpose of avoiding tax-related penalties under federal, state or local tax law or promoting, marketing or recommending to another party any transaction or matter addressed therein.

EXHIBIT 22

AMERICAN ARBITRATION ASSOCIATION

THOMAS DEUTSCH, ESQ.,

Claimant,

CASE NO. 01-20-0014-3715

v.

MICROSOFT CORPORATION,

Respondent.

FOURTH AMENDED CLAIM

Claimant, Thomas Deutsch, Esq., provides this FOURTH Amended Claim to update and amend the Amended Claim that was filed on or about March 12, 2021.

Statement of Facts

On or around October 17, 2019, Claimant purchased Microsoft OneDrive as part of a ‘Microsoft 365 Personal’ service subscription (“365 Service”) through Apple to ensure his documents, data and backups were always available to him in the cloud, as advertised and promised via contract by Microsoft. The 365 Service was delivered to Claimant entirely electronically. Apple had and still has clear authority to contract on behalf of Microsoft and charged Claimant’s credit card immediately upon Claimant’s contract with Microsoft for a subscription to this service. At the time Claimant paid for Claimant’s Microsoft 365 Personal subscription, no terms of service such as the Microsoft Services Agreement (the “MSA”) were presented to Claimant, nor did Claimant agree with the MSA, implicitly or explicitly, as part of Claimant’s contract with Microsoft at the time of payment. For every month from October 17, 2019 through the date of this filing, Claimant’s credit card has continued to be charged \$6.99 plus taxes for Claimant’s 365 Service.

After subscribing and immediately transferring all of his documents, data and backups onto OneDrive, Claimant spent a great deal of time reorganizing Claimant’s files on OneDrive as well as continuing to add and modify documents, data and backups. Claimant used OneDrive as a cloud backup for all of his documents, data and backups for his personal Dell desktop computer at his residence (the “Desktop”) and the Photos folder on his iPhone.

Sometime in the spring, 2020, Claimant began to get a message on his computer that he needed to re-log into OneDrive. Claimant attempted to do so multiple times over the span of

weeks, but the OneDrive help login continued to send Claimant to an error screen. At no point was Claimant notified that his account had been disabled nor was Claimant notified that his documents were no longer being backed up onto OneDrive.

Claimant contacted Microsoft three times in writing through their help system, but never received a reply after weeks of attempting to contact Microsoft. Finally, Claimant received an email on May 27, 2020 (the “May 27th Email”) informing Claimant that his OneDrive account access had been disabled “due to a serious violation of the Microsoft Services Agreement.” This was the first time Claimant had been presented or seen the MSA.

The May 27th Email also relayed that, “Microsoft will immediately cease charging the credit card on file for recurring charges.” In direct contravention to the MSA and the May 27th Email, Claimant’s credit card has been charged the contractual \$6.99 plus taxes charge in each month since the May 27th Email through the date of this filing.

On June 1, 2020, Claimant completed a Notice of Dispute and mailed a hard copy to Microsoft’s specified address and replied to the May 27th Email with a copy of the Notice of Dispute. To date, Claimant has not received any response from the Microsoft “CELA Arbitration” unit that is specified in the Notice of Dispute. Although the MSA contractually obliges Microsoft to engage in good faith efforts to resolve a dispute with a user, Microsoft took no efforts to resolve Claimant’s concerns, let alone engage in good faith efforts to do so.

After Claimant further requested his account be reactivated and further information on why Claimant’s account had been disabled, Claimant received an email on June 5, 2020 (the “June 5th Email”) from a Relationship Manager also reiterating the unsubstantiated allegation that Claimant had committed a “serious violation” of the MSA, but then went further to say that Claimant’s account “was properly closed.” The June 5th Email contradicted earlier representations by Microsoft – specifically, in the May 27th Email – which indicated that Claimant’s account had been “disabled”. The June 5th Email also stated that “Pursuant to our terms, we cannot reactivate your account, nor provide details as to why it was closed.” Nowhere in the MSA does it specify that Microsoft cannot or would not provide details as to why an account is closed. The June 5th Email goes further to say that “This represents Microsoft’s final communication regarding this account.” Microsoft’s MSA further specifies that Claimant had to wait 60 additional days before Claimant could avail himself of any relief through state court litigation or arbitration. Microsoft specifies that ‘waiting period’ is to provide an opportunity for Microsoft to attempt to reconcile the dispute in good faith.

Shortly after the June 5th Email, while Claimant was waiting for Microsoft to respond to Claimant to resolve his dispute over the disabled OneDrive account, Claimant attempted a customary Microsoft update of his Windows 10 operating system on his Desktop. Claimant has two hard drives in his Desktop; one is a solid start hard drive (the “SSD”) that allows for faster processing of programs, the other is a ‘regular’ hard drive that has slower processing speeds, but much larger storage capacity. As Claimant was updating Windows, the SSD reached its full capacity, but instead of warning the Claimant that the disk space was exhausted, the update program continued to attempt to update, which effectively ceased all Windows functioning and

generated the attached Exhibit 1, which is commonly and colloquially termed the Microsoft Windows 10 “Blue Screen of Death.”¹ As a practical matter, the Blue Screen of Death causes a computer to freeze without access to Windows, and necessitates a reinstallation of Windows, which erases the hard drive and all files and programs saved to the computer.

Two career IT professionals and the Claimant spent dozens of hours attempting to reinstall Microsoft Windows from the original operating system disc from Dell and online sources in response to the Blue Screen of Death, but when Windows was ultimately reinstalled, all of Claimant’s documents, data, backups, and programs had been purged from Claimant’s SSD. One of Claimant’s IT professionals installed and ran the Stellar Data Recovery program in an attempt to recover Claimant’s documents, data, backups or programs, but all of the files the program recovered were ‘corrupted’ when Claimant attempted to open them.

Thereafter, on June 24, 2020, Claimant received an email from Microsoft that specified that Claimant’s “support case has been closed.”

After not hearing anything from Microsoft’s “CELA Arbitration” unit or any other unit or individual from Microsoft, Claimant filed the Consumer Demand for Arbitration before the AAA on August 14, 2020 in an effort to restore Claimant’s access to his entire set of documents, data and backups.

Through the date of this filing, Microsoft has refused any resolution that would allow Claimant to access even one of his documents, data or backups, even after Claimant offered to waive in writing any and all claims against Microsoft even if Microsoft chose to use PhotoDNA or any other technology to scan Claimant’s entire set of documents, data and backups for child sexual exploitation and abuse imagery (“CSEAI”) prior to allowing Claimant to retrieve them.

Analysis

As a direct consequence of the combination of Microsoft’s refusal to allow Claimant access to his OneDrive account and Microsoft’s defective Windows 10 updating system that creates the Blue Screen of Death that wiped out Claimant’s hard drive backups, Claimant currently only has his personal documents, data and backups as of October, 2019 with no updates to those documents or their organization or any additional documents that were created or acquired after that date. That loss represents thousands of hours of Claimant’s time creating, revising and organizing all of Claimant’s computer records from his entire life. As a meticulous attorney, the damages from that loss to Claimant are appreciably greater than the average computer user and a number of those documents are sensitive attorney-client privileged documents from pro bono cases and other personal legal services Claimant has provided to family members and acquaintances. Most of those documents, data and backups, which number into the thousands, are irretrievable from any other source, with Microsoft now possessing the only readable digital copies remaining. Claimant continues to suffer significant and irreparable harm from not having access to his comprehensive set of organized documents, data and backups.

¹ For additional background on the Blue Screen of Death, see https://en.wikipedia.org/wiki/Blue_screen_of_death.

At no time prior to Respondent's Answer on September 15, 2020, over four months after Claimant's account had been disabled, was Claimant aware or informed that Microsoft was alleging that Claimant had shared CSEAI via OneDrive. Moreover, at no time was Claimant aware or informed that Microsoft was scanning every document, data and backup Claimant was sharing in private and/or public settings.

Claimant flatly rejects Microsoft's baseless allegation that Claimant possessed and/or shared any CSEAI imagery via OneDrive. As to public sharing, Claimant asserts he has not publicly shared any document, data or imagery via OneDrive onto public venues such as Facebook, Twitter, Instagram, etc. as Claimant did not share any document, data or imagery publicly from any source onto any public venue since prior to October 2019.

As will be further detailed below, Microsoft does not "balance the privacy of its customers against the company's legitimate business interest," as they contend in their Answer (see page 1). In fact, the European Union, as of December 20, 2020, banned Microsoft from using detection software on customers' private documents, precisely as Microsoft used PhotoDNA software on Claimant's images, because Microsoft and other similar technology providers do not balance their customers interests appropriately.²

Specific to this Claim, Microsoft attempts a narrative that Microsoft has lofty goals of wearing a white hat to prevent the sharing of CSEAI. But in every argument Microsoft makes, they demonstrate that their primary aim is to keep streamlined policies and procedures in place that minimize their own administrative expenses and legal conveniences with little, if any, regard to the contractual rights that Microsoft owes to their OneDrive customers and counterparties.

Claimant presents the below Bases for the relief requested at the conclusion of this Second Amended Claim. Claimant asserts the following Bases, but in so doing, in no way assumes the burden of proof of any element or claim for which the burden of proof properly remains with the Respondent. Claimant further reserves the right to amend or supplement these Bases as his investigation and this case proceed.

These bases include:

- I. Claimant Did Not Possess or Share CSEAI VIA OneDrive
- II. Breach of Contract
- III. Breach of Implied Covenant of Good Faith and Fair Dealing
- IV. Negligence
- V. Breach of Privacy
- VI. Conversion
- VII. The MSA's Limitation on Liability Should Not Be Enforced
- VIII. Microsoft Acted in Bad Faith
- IX. Microsoft Violated New Jersey Consumer Protection Laws
- X. The MSA's Class Action Waiver Should Not Be Enforced

² See [Europe's ePrivacy Rule Would Limit the Hunt for Online Child Sex Abuse - The New York Times \(nytimes.com\)](https://www.nytimes.com/2020/12/20/technology/eu-privacy-rule-child-sex-abuse.html)

I. Claimant Did Not Possess and/or Share CSEAI Via OneDrive

A. Microsoft Has Not Provided Any Evidence that Claimant Possessed or Shared CSEAI

Claimant vehemently denies that he possessed or shared CSEAI. Despite countless requests from Claimant and counsel for Claimant, Microsoft has failed to produce any direct evidence that Claimant possessed or shared CSEAI. Rather, Microsoft has simply relied on self-serving, conclusory statements. Moreover, as of the date of this Second Amended Claim, counsel for Microsoft have indicated that they have not seen the alleged image that Microsoft flagged as CSEAI, nor has an independent third party verified Microsoft's allegation that Claimant possessed or shared CSEAI.

Microsoft further affirmed that the company submitted the alleged CSEAI to the Cyber Tipline so that law enforcement authorities could investigate the claim. However, over one year after Microsoft submitted the alleged CSEAI to the authorities, there has been no indication whatsoever that the federal government—the entity charged with determining whether an image is in fact a violation of federal law—has made any inquiry into the alleged offending image. Claimant has received no correspondence or been contacted by any entity regarding the offending image, which further supports Claimant's position that Microsoft's PhotoDNA reported a false positive for a CSEAI Image. Claimant is willing to submit to a background search to demonstrate that no charges have been filed against him for CSEAI imagery (or any other crime in his life beyond a speeding ticket).

B. Claimant Did Not Share Any Images Via OneDrive on May 12, 2020

Microsoft alleges that Claimant shared a CSEAI image via his OneDrive account on May 12, 2020. In the MSA and filings for this arbitration, Microsoft makes clear that it runs its PhotoDNA software only on documents and images shared via OneDrive. In this case, Claimant did not share *any* images via OneDrive on May 12, 2020, let alone alleged CSEAI, as Microsoft alleges. In fact, Claimant only has shared eight documents total in his eight months of access to OneDrive, none of which was on May 12, 2020, the date that Microsoft alleges was the date Claimant shared CSEAI via his OneDrive account. A current screen shot of Claimant's OneDrive iPhone app 'share summary' is attached hereto as Exhibit 2.

C. Microsoft's PhotoDNA Very Likely Reported a False Positive for a CSEAI Image on Claimant's Account

Microsoft's PhotoDNA is not a flawless technology and commonly generates false positive detections for CSEAI from no less than four general sources:

1. **Hash issues**—Microsoft is not actually ‘scanning’ through files as one might assume from Respondent’s Answer. Instead, Microsoft’s PhotoDNA creates a ‘hash’³ of those files, which is effectively a randomized recreation. PhotoDNA works like an antivirus product where it looks for signatures of inappropriate content. The PhotoDNA software works through the same process so it doesn’t actually look at the illegal content Microsoft is attempting to detect. But just like an antivirus product, this process is prone to significant errors.⁴ Generating the hash and ensuring the original picture is inappropriate creates hashes being close to a potential CSEAI, but not actually a real match.
2. **Wrong account**—PhotoDNA can make a mistake with whose account the image is contained in.
3. **Incorrect content flagged**—PhotoDNA can flag a legal image as illegal. In Sean Davis’ Affidavit in Support of Respondent’s Opposition, he specifically articulates that “if an image has been resized, recolored, saved in a different file format or otherwise similarly altered, Photo DNA can still reliably identify copies of the image when other hashing technologies (that require every file characteristic to be precisely the same) could not.” In effect, an illegal image may have been modified to make it a legal image, but PhotoDNA’s hashing technology would still flag the image as illegal CSEAI precisely because the “signature is based on the essence of the image.”
4. **Other programming errors**—PhotoDNA, like any other computer program, can contain any number of other errors. The program can catch old data, scan incorrect places, etc. The possibilities of various kinds of programming errors are endless. To attempt to control the error checking process in its software, Microsoft has a department called QA or Testing. But Microsoft has had historically very poor performance in their QA. For example, their product updates often get revoked.⁵

II. Breach of Contract

A. Standard

To succeed on a breach of contract claim, a claimant must demonstrate that the parties entered into a valid contract, the defendant failed to perform their obligations under the contract, and that the claimant suffered damages as a result of defendant’s breach. *See, e.g., Murphy v Implicito*, 920 A.2d 678, 689 (N.J. App. Div. 2007).

³ See [Hash Definition \(techterms.com\)](https://techterms.com/definition/hash)

⁴ More information on the antivirus hash issues discussing how problematic false positives are in this type of detection process can be found here:
<https://www.pcworld.com/article/2883692/virustotal-tackles-false-positive-malware-detections-plaguing-antivirus-and-software-vendors.html>

⁵ A discussion by one of Microsoft’s own former engineers can be found here:
<https://borncity.com/win/2019/09/25/ex-microsoftler-erklrt-die-schlechte-windows-10-qualitt/>

B. Microsoft Breached the MSA Because It Failed to Provide Claimant Access to His Documents

The reason that Claimant contracted with Microsoft was for Microsoft to provide a cloud backup of Claimant's files in case anything would happen to Claimant's files on his personal devices. Claimant has been paying a monthly service fee under the terms of his contract with Microsoft, a fee that Microsoft continues to collect as of the date of this Second Amended Claim. Claimant has made countless requests to obtain access to his files, but Microsoft has failed to provide Claimant with access to a single one of his files. This represents a material breach of the contract between Claimant and Microsoft. Claimant has suffered extensive damages because of the breach, which include, but are not limited to, fees for the Microsoft service, economic and other harm due to the inability to access his documents, and costs and attorneys' fees to bring this action to enforce the terms of the agreement.

C. Microsoft Breached the MSA Because It Failed to Follow Its Own Policy on When Claimant's Documents Are Scanned by PhotoDNA

The terms of the agreement between Claimant and Microsoft specify that Microsoft will utilize PhotoDNA only on documents that Claimant shares via OneDrive. At no time did Claimant share images, CSEAI or otherwise, via OneDrive on May 12, 2020. Rather, Microsoft has utilized PhotoDNA to scan Claimant's files beyond that permitted by the MSA. By scanning Claimant's files outside of that permitted by the MSA, Microsoft has breached the MSA. This represents a material breach of the contract between Claimant and Microsoft. Claimant has suffered extensive damages because of the breach, which include but are not limited to, fees for the Microsoft service, economic and other harm due to the inability to access his documents, and costs and attorneys' fees to bring this action to enforce the terms of the agreement.

D. Microsoft Breached the MSA Because It Did Not Undertake Efforts to Try to Resolve Claimant's Request Before the Arbitration Demand

The MSA provides at the beginning of Section 15 that "We hope we never have a dispute, but if we do, you and we agree to try for 60 days to resolve it informally." Hence, the terms of the agreement between Claimant and Microsoft specify that Microsoft will undertake efforts to try to resolve disputes prior to arbitration. Microsoft made no efforts, let alone a good faith attempt, to try to resolve this dispute prior to Claimant's demand for arbitration. By failing to take any efforts, let alone good faith efforts, to try to resolve this dispute prior to Claimant's demand for arbitration, Microsoft has breached the MSA. This represents a material breach of the contract between Claimant and Microsoft. Claimant has suffered extensive damages because of the breach, which include but are not limited to, fees for the Microsoft service, economic and other harm due to the inability to access his documents, and costs and attorneys' fees to bring this action to enforce the terms of the agreement.

E. Microsoft Breached the MSA Because It Charged Claimant for OneDrive Service After Terminating Claimant's Account

The MSA provides in Section 9d. "Recurring Payments. When you purchase the Services on a subscription basis (e.g. monthly, every 3 months or annually), you agree that you are authorizing recurring payments, and payments will be made to Microsoft by the method and at the recurring intervals you have agreed to, until the subscription for that Service is terminated by you or by Microsoft." Hence, the terms of the agreement between Claimant and Microsoft specify that if Microsoft terminates a customer's OneDrive account, Microsoft will cease the authorization of recurring payments. For Claimant, Microsoft terminated his account, but continued to authorize charges against Claimant for OneDrive services. In fact, as of the date of this Second Amended Claim, and despite months of ongoing arbitration, Microsoft continues to authorize recurring charges for Claimant's OneDrive account. By failing to terminate the authorization of recurring charges for Claimant's OneDrive account, Microsoft has breached the MSA. This represents a material breach of the contract between Claimant and Microsoft. Claimant has suffered extensive damages because of the breach, which include but are not limited to, fees for the Microsoft service, economic and other harm due to the inability to access his documents, and costs and attorneys' fees to bring this action to enforce the terms of the agreement.

F. Microsoft Breached the EULA Because It Provided Defective Windows Software Update Process

Microsoft guarantees that it will provide Microsoft Windows updates that will terminate if a person's computer does not have sufficient memory to fully download the update. Microsoft's policy on the update program to Windows 10 is clear,

"Windows 10 updates provide the latest features and security improvements to help keep your PC more current and more secure. Before the installation process starts, Windows checks to make sure there's enough storage space on your device for the installation process and for these new features and security improvements.

*If there isn't enough open space on your internal drive, you'll see a message (like the one below) that tells you Windows requires more space."*⁶

According to, and in reliance upon, Microsoft, the Claimant used the update program that should have stopped and not let Windows updater continue with the update process.

This safeguard endeavors to ensure that a Microsoft Windows update does not push the operating system into the Blue Screen of Death. Here, when Claimant attempted to install a routine Microsoft Windows 10 update, his SSD hard drive did not have sufficient memory to install the update. Rather than pause the update and alert Claimant that his SSD was at out of memory, Microsoft's update attempted to complete its update even though the SSD memory wasn't sufficient to download the full update. As a direct result of Microsoft's 10 update flaw, Windows crashed into the Blue Screen of Death, which eliminated Claimant's access to his

⁶ [Free up space for Windows 10 updates \(microsoft.com\)](https://www.microsoft.com/windows/windows-10-updates)

operating system and his computer's contents. The only solution after weeks of attempts to reboot the existing Windows 10 application was to reinstall Windows 10. Reinstalling Windows had the effect of erasing all of Claimant's applications, documents, data and backups on his SSD drive. This represents a material breach of the agreement between Claimant and Microsoft on Windows updates. Claimant has suffered extensive damages because of the breach, which include but are not limited to, economic and other harm due to the inability to access his documents and programs, and costs and attorneys' fees to bring this action to enforce the terms of the agreement.

III. Breach of Implied Covenant of Good Faith and Fair Dealing

A. Standard

A covenant of good faith and fair dealing is implied in every contract in New Jersey. *Sons of Thunder, Inc. v. Borden, Inc.*, 148 N.J. 396, 420, 690 A.2d 575 (1997). Implied covenants are as effective components of an agreement as those covenants that are express. *Aronsohn v. Mandara*, 98 N.J. 92, 100, 484 A.2d 675 (1984). Although the implied covenant of good faith and fair dealing cannot override an express term in a contract, a party's performance under a contract may breach that implied covenant even though that performance does not violate a pertinent express term. *Sons of Thunder, Inc.*, *supra*, 148 N.J. at 419, 690 A.2d 575.

Unlike many other states, in New Jersey "a party to a contract may breach the implied covenant of good faith and fair dealing in performing its obligations even when it exercises an express and unconditional right to terminate." *Id.* at 422, 690 A.2d 575; *see also Bak-A-Lum Corp. v. Alcoa Bldg. Prods., Inc.*, 69 N.J. 123, 129–30, 351 A.2d 349 (1976) (finding that defendant's conduct in terminating contract constituted bad faith although conduct did not violate express terms of written agreement).

The Restatement (Second) of Contracts notes that every contract imposes on each party a duty of good faith and fair dealing in its performance and enforcement. *Restatement (Second) of Contracts* § 205 (1981). A comment to the Restatement states that "[g]ood faith performance or enforcement of a contract emphasizes faithfulness to an agreed common purpose and consistency with the justified expectations of the other party; it excludes a variety of types of conduct characterized as involving 'bad faith' because they violate community standards of decency, fairness or reasonableness." *Restatement (Second) of Contracts* § 205 comment a (1981). Under New Jersey law, "[i]n every contract there is an implied covenant that neither party shall do anything which will have the effect of destroying or injuring the right of the other party to receive the fruits of the contract; which means that in every contract there exists an implied covenant of good faith and fair dealing." *Sons of Thunder, Inc.*, *supra*, 148 N.J. at 419, 690 A.2d 575.

As New Jersey courts have recognized, "[a] contract thus would be breached by a failure to perform in good faith if a party uses its discretion for a reason outside the contemplated range—a reason beyond the risks assumed by the party claiming the breach." *Wilson v. Amerada Hess Corp.*, 168 N.J. 236, 246 (2001). For example, when one party to a contract maintains discretion to terminate service, it cannot be "unbridled discretion." *Id.* at 250. A party breaches

the implied covenant of good faith and fair dealing when it exercises its discretion “arbitrarily, unreasonably, or capriciously, with the objective of preventing the other party from receiving its reasonably expected fruits under the contract.” *Id.* at 251.

B. Microsoft Has Breached the Implied Covenant of Good Faith and Fair Dealing

Microsoft’s unilateral actions to terminate Claimant’s access to his documents violates New Jersey’s implied covenant of good faith and fair dealing. Microsoft scanned Claimant’s files outside of the scope of contractually-eligible scannable files, has not provided any evidence to substantiate its allegation that Claimant shared CSEAI via OneDrive, and has not provided any evidence that Claimant possessed CSEAI. Moreover, Microsoft has not provided any evidence of human review of the image that was flagged by its PhotoDNA software. On top of all of this, counsel for Microsoft have taken the remarkable position of stating that, even if Microsoft incorrectly flagged CSEAI in Claimant’s account, and even if Microsoft were negligent in its human review of the flagged image, Claimant still would not be entitled to *any* relief.

This type of corporate behavior – unilateral, arbitrary, unreasonable, reckless, and in wanton disregard of a customer’s rights – is precisely the conduct that New Jersey courts have found violative of the implied covenant of good faith and fair dealing.

Microsoft’s proposed interpretation of the 365 Service contract is entirely inapposite to every aspect of marketing representations that Microsoft makes regarding OneDrive, which are incorporated as part of the contractual understanding. Claimant signed up for the OneDrive service relying on Microsoft’s advertisement that Claimant’s files and their organization for “Any file, anywhere, always protected,” which is the Microsoft landing/advertising page for OneDrive. Claimant had a strong and reasonable belief that his files were safe from loss, which is precisely what Microsoft’s intent is in their OneDrive advertising.

Microsoft also advertises that they, “Back up and protect. If you lose your device, you won’t lose your files and photos when they’re saved in OneDrive.” Also, while using OneDrive, Microsoft continually refers to Claimant’s documents being “Always” backed up once they are uploaded to OneDrive. Microsoft clearly advertises OneDrive as “Always” backing up documents and having them available to users “anytime” and on “any device.” No asterisks or disclaimers are ever used on what would amount to false advertising if Microsoft could indeed be allowed to prevent users from accessing their own documents. No user would ever reasonably expect that by signing up for Microsoft’s OneDrive that the biggest risk to that user losing the thousands of hours creating, revising and organizing their documents, data and backups is Microsoft’s unilateral decision making to intentionally deprive that user of his access to his own files due to false positives from a computer software program that Microsoft knows to be less than 100% accurate.

Microsoft has a laudable policy goal of reducing the sharing of CSEAI, but in practice, they are seeking to streamline their administrative expenses through bad faith construction of their resolution policies at the expense of their contractual obligations to their consumers. Microsoft has no effective adjudication procedure for resolving whether they have a false

positive from PhotoDNA and in doing so, Microsoft deprives their customers of any meaningful opportunity to dispute contractual violations. Their intentional construction of this resolution policy (or the lack thereof) in practice and in the MSA itself violates the implied covenant of good faith and fair dealing.

Claimant's situation illustrates well: Nearly ten months have elapsed since Claimant was blocked from accessing his entire set of documents, data and backups and there still appears to be no one in the entire Microsoft company or their outside counsel who has seen an alleged CSEAI and considered any of Claimant's objections.

Microsoft acts as both defendant and judge in their practice in that they asserted a unilateral right to be judge, jury and enforcer. Microsoft is fully aware that their PhotoDNA system is not a perfect system and that errors, particularly false positives, are detected by the system. Microsoft applies the extreme sanction of blocking access to documents before there is any attempt to adjudicate or resolve whether a violation has actually ever occurred. Microsoft provides no meaningful chance to correct their mistakes, or a customer's if inadvertent. The June 5th email from Microsoft communicating "This represents Microsoft's final communication regarding this account" could not better illustrate the point that Microsoft has no interest in providing any meaningful opportunity to adjudicate.

By their very definitions, terms like "inappropriate" and "objectionable" in the MSA are subjective, not objective, standards. Here, as in other instances, Microsoft compels customers to wait 60 days before they can even file for arbitration, even though Microsoft has made zero effort whatsoever to resolve Claimant's challenges in that period. Even to the day of this filing, neither Microsoft nor their outside counsel has even gone back to check whether the alleged image is in fact CSEAI. For all of the foregoing reasons, Microsoft has breached the implied covenant of good faith and fair dealing. Claimant has suffered extensive damages because of the breach, which include but are not limited to, economic and other harm due to the inability to access his documents, and costs and attorneys' fees to bring this action.

IV. Negligence

A. Standard

To succeed upon a cause of action for negligence, a plaintiff must demonstrate the existence of "(1) a duty of care, (2) a breach of that duty, (3) actual and proximate causation, and (4) damages." *Jersey Cent. Power & Light Co. v. Melcar Util. Co.*, 212 N.J. 576, 594, 59 A.3d 561 (2013).

B. Microsoft Breached its Duty to Apply and Enforce the MSA in a Reasonable Manner

Microsoft maintains great discretion under the MSA to terminate a customer's access to their documents. Given the broad language in the MSA, which is a contract of adhesion and affords customers no reasonable chance of negotiation, among its obligations and duties, Microsoft has a duty to apply and enforce its discretion in a reasonable manner. Microsoft

breached its duty to apply and enforce its discretion in a reasonable manner when it improperly flagged Claimant's account as containing CSEAI, and failed to conduct a reasonable human review of the PhotoDNA scan to ensure that the alleged image was not a false positive for CSEAI. Microsoft's acts and omissions are both an actual and proximate cause of harm to Claimant, which includes but is not limited to Claimant's inability to access and utilize his documents. Claimant has suffered extensive damages because of the breach, which include but are not limited to, economic and other harm due to the inability to access his documents, and costs and attorneys' fees to bring this action.

C. Microsoft Breached its Duty to Scan Only Those Documents that Claimant Shares Via OneDrive

Among its obligations and duties, Microsoft has a duty to act in a reasonable manner and follow its own policies. One such policy is that Microsoft states it will not scan a customer's private files unless those files are shared via OneDrive. Microsoft breached its duty with respect to Claimant because Microsoft scanned Claimant's files that were not shared via OneDrive, thus breaching a Microsoft policy. Microsoft's acts and omissions are both an actual and proximate cause of harm to Claimant, which includes but is not limited to Claimant's inability to access and utilize his documents. Claimant has suffered extensive damages because of the breach, which include but are not limited to, economic and other harm due to the inability to access his documents, and costs and attorneys' fees to bring this action.

D. Microsoft Breached its Duty to Take Good Faith Efforts to Try to Resolve Claimant's Request Before Filing Arbitration

Among its obligations and duties, Microsoft has a duty to act in a reasonable manner and follow its own policies. One such policy is that Microsoft states it will take good faith efforts to try to resolve disputes prior to arbitration. Microsoft made no efforts, let alone a good faith attempt, to try to resolve this dispute prior to Claimant's demand for arbitration. By failing to take any efforts, let alone good faith efforts, to try to resolve this dispute prior to Claimant's demand for arbitration, Microsoft has breached its duty. Microsoft's acts and omissions are both an actual and proximate cause of harm to Claimant. Claimant has suffered extensive damages because of the breach, which include but are not limited to, fees for the Microsoft service, economic and other harm due to the inability to access his documents, and costs and attorneys' fees to bring this action to enforce the terms of the agreement.

E. Microsoft Breached its Duty to Provide Microsoft Windows Updates that Are Not Defective

Among its obligations and duties, Microsoft has a duty to act in a reasonable manner and follow its own policies. One such policy is that Microsoft states it will create Windows 10 updates that auto-stop and create an alert if a user's computer does not have sufficient memory to install the update. Microsoft breached its duty with respect to Claimant because Microsoft provided Claimant with a Microsoft Windows 10 update that did not maintain a safeguard that pauses the updated in the event a user's hard drive does not have sufficient memory to install the update. When Claimant was installing the update provided by Microsoft, his SSD drive did not

have sufficient memory to install the update. But, the update did not stop. Rather, it crashed Claimant's computer, which necessitated a Windows reinstallation, causing Claimant to lose all the programs, documents, data and backups saved on his SSD drive. Microsoft's acts and omissions are both an actual and proximate cause of harm to Claimant, which includes but is not limited to Claimant's inability to access and utilize his documents. Claimant has suffered extensive damages because of the breach, which include but are not limited to, economic and other harm due to the inability to access his documents, and costs and attorneys' fees to bring this action.

V. Breach of Privacy

A. Standard

Under New Jersey law, a breach of privacy occurs where a defendant "intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns ... if the intrusion would be highly offensive to a reasonable person." This determination turns on whether plaintiff had a reasonable expectation of privacy. *White v. White*, 344 N.J.Super. 211, 222, 781 A.2d 85 (Ch.Div.2001).

B. Microsoft Breached Claimant's Privacy When the Company Scanned Claimant's Documents Without His Consent

Claimant did not grant Microsoft the ability to scan his personal documents unless the documents were shared via OneDrive. Moreover, Microsoft itself affirms that the company will not scan a user's files unless the files are shared via OneDrive. This is to protect the privacy of users. As such, Claimant had a reasonable expectation of privacy in the documents he stored with Microsoft that were not shared via OneDrive.

Microsoft breached Claimant's privacy when the company scanned Claimant's documents that were not shared via OneDrive, without his consent. Microsoft's conduct was intentional, in that the company structured its software programs to scan Claimant's files. This type of intrusion into one's personal files would be highly offensive to a reasonable person, and in fact was highly offensive to Claimant and caused him significant harm and damages.

Microsoft's acts and omissions are both an actual and proximate cause of harm to Claimant, which includes but is not limited to Claimant's inability to access and utilize his documents. Claimant has suffered extensive damages because of the breach, which include but are not limited to, economic and other harm due to the inability to access his documents, and costs and attorneys' fees to bring this action.

VI. Conversion

A. Standard

Conversion is the intentional exercise of dominion and control over chattel that seriously interferes with the right of another to control that chattel. *See, e.g., Chi. Title*, 409 N.J. Super. at

454, 978 A.2d 281 (citing Restatement (Second) of Torts § 222A(1)). Where possession is initially lawful, it is not tortious unless and until the possessor acts in a way that conflicts with the true owner's rights. Temple Co., 69 N.J.L. at 37, 54 A. 295. The demand is the linchpin that transforms an initial lawful possession into a setting of tortious conduct. A claimant must make a demand “at a time and place and under such circumstances as defendant is able to comply with if he is so disposed, and the refusal must be wrongful.” Mueller, 8 N.J. at 207, 84 A.2d 620.

Importantly, courts have recognized that conversion claims can be brought for computer files. *See, e.g., Thyroff v. Nationwide Mutual Insurance Co.*, 8 N.Y.3d 283, 832 N.Y.S.2d 873, 864 N.E.2d 1272 (N.Y.2007).

B. Microsoft’s Wrongful Refusal to Return Claimant’s Files Constitutes Conversion

Claimant provided Microsoft with a copy of all of his files so that Microsoft could hold the files as backup storage in trust for Claimant. When Claimant sought to retrieve his files from Microsoft, the company refused, and for months did not even provide Claimant with a reason for the refusal. Several months later, after countless inquiries by Claimant, Microsoft alleged that Claimant shared CSEAI via his OneDrive account, but did not provide any evidence to corroborate the allegation. To this day, Claimant has repeatedly demanded the return of his documents, and Microsoft has intransigently refused. Microsoft has asserted they have been able to comply with Claimant’s request, but has refused. Microsoft’s actions and omissions amount to conversion. Claimant has suffered extensive damages, which include but are not limited to, economic and other harm due to the inability to access his documents, and costs and attorneys’ fees to bring this action

VII. The MSA’s Limitation on Liability Should Not Be Enforced

A. Standard

New Jersey courts have not hesitated to strike limited liability clauses that are unconscionable or in violation of public policy. *Moreira Constr. Co., Inc. v. Moretrench Corp.*, 97 N.J.Super. 391, 394, 235 A.2d 211 (App.Div.1967), *aff’d*, 51 N.J. 405, 241 A.2d 236 (1968). There is no hard and fast definition of unconscionability. As the New Jersey Supreme Court explained in *Kugler v. Romain*, 58 N.J. 522, 279 A.2d 640 (1971), unconscionability is “an amorphous concept obviously designed to establish a broad business ethic.” *Id.* at 543, 279 A.2d 640. The standard of conduct that the term implies is a lack of “good faith, honesty in fact and observance of fair dealing.” *Id.* at 544, 279 A.2d 640.

In determining whether to enforce the terms of a contract, a court looks not only to its adhesive nature, but also to “the subject matter of the contract, the parties’ relative bargaining positions, the degree of economic compulsion motivating the ‘adhering’ party, and the public interests affected by the contract.” *Rudbart v. North Jersey District Water Supply Comm’n*, 127 N.J. 344, 356, 605 A.2d 681, *cert. denied*, 506 U.S. 871, 113 S.Ct. 203, 121 L.Ed.2d 145 (1992). Where the provision limits a party’s liability, a court must pay particular attention to any inequality in the bargaining power and status of the parties, as well as the substance of the

contract. *Valhal Corp. v. Sullivan Assoc., Inc.*, 44 F.3d 195, 204 (3rd Cir.1995); *Marbro, Inc. v. Borough of Tinton Falls*, 297 N.J.Super. 411, 416–18, 688 A.2d 159 (Law Div.1996).

A court also focuses on whether the limitation is a reasonable allocation of risk between the parties or whether it runs afoul of the public policy disfavoring clauses which effectively immunize parties from liability for their own negligent actions. *Valhal, supra*, 44 F.3d at 202–04; *Marbro, supra*, 297 N.J.Super. at 416–18, 688 A.2d 159. To be enforceable, the amount of the cap on a party’s liability must be sufficient to provide a realistic incentive to act diligently. *Valhal, supra*, 44 F.3d at 204; *Marbro, supra*, 297 N.J.Super. at 416, 688 A.2d 159.

B. The Limited Liability Provision Should Not Be Enforced

Claimant respectfully submits that the MSA’s limited liability provision should not be enforced. The MSA is a classic contract of adhesion, where Microsoft has grossly unequal bargaining power in comparison to Claimant and other users. In fact, Microsoft offers the MSA on a take-it-or-leave-it basis, another factor that supports the contention that the MSA is a contract of adhesion.

Perhaps more importantly, the limit on liability eviscerates the contract and its fundamental purpose because Microsoft’s potential damages are so nominal that it has the practical effect of allowing Microsoft to avoid responsibility for negligence, breach of contract, breach of privacy, conversion, or other harms. Microsoft and their counsel assert that Microsoft would only be liable under the MSA to return the amounts Claimant has paid for the 365 Service since he started his subscription. For the period of October 20, 2019 through March 20, 2021, that would amount to \$118.83 (the multiplication of 17 months times \$6.99 per month). Such a broad shield is contrary to the public policy of New Jersey, which is to provide consumers with adequate protections in their privacy and property. Moreover, that absurd limit on liability provides no realistic incentive for Microsoft to act diligently, or even in good faith, because Microsoft asserts they have only \$118.83 of risk under their designed limitation of liability, which explains much of their corporate and legal behavior to date — for example, not taking good faith efforts to resolve this dispute pre-arbitration and/or not applying a reasonable human review process to verify that the alleged image is CSEAI. Here, Microsoft violated Claimant’s privacy and has confiscated his property – all of his documents, data and backups. Under these circumstances, the limited liability provision is unconscionable and thus should not be enforced. See, e.g., *Lucier v. Williams*, 366 N.J.Super. 485, 493 (2004).

C. Microsoft’s Acts and Omissions Qualify as Bad Faith Corporate Conduct and are in Wanton Disregard of Claimant’s Rights

Microsoft’s egregious acts and omissions unquestionably qualify as Bad Faith corporate conduct and are in wanton disregard of Claimant’s rights. In 2019 alone, Microsoft reported over \$125 billion in revenue.⁷ Despite massive revenues that place Microsoft as one of the wealthiest companies in the world, Microsoft is cavalierly unresponsive in its handling of legitimate consumer concerns. With respect to Claimant, Microsoft has unabashedly violated several terms

⁷ See [Microsoft 2019 Annual Report](#) (last accessed March 4, 2021)

of the MSA and otherwise has engaged in egregious, reckless, and unlawful conduct. When faced with this Claim, counsel for Microsoft have taken the outrageous position that, *even if* Microsoft wrongly flagged Claimant for CSEAI, *and even if* Microsoft has breached several terms of the MSA, *and even if* Microsoft was negligent in handling Claimant's request, *then still nevertheless* the company is immune from liability due to liability shields and the limited liability provisions in the MSA. This reckless corporate conduct, which is in wanton disregard for Claimant's rights, is something that Microsoft calculates it can get away with due to the grossly one-sided provisions in the MSA, a contract of adhesion. Claimant respectfully submits that the limited liability provision be held unenforceable, and that the Arbitrator award Claimant compensatory, exemplary and/or punitive damages. Moreover, as the Supreme Court of New Jersey has held, in the face of wrongful corporate conduct, the wealth of the defendant is a proper consideration in setting a damage award. *See, e.g., Herman v. Sunshine Chemical Specialties, Inc.*, 133 N.J. 329, 339 (1983).

VIII. Microsoft Acted in Bad Faith

In addition to the numerous ways described above, Claimant also specifically alleges Microsoft has and is acting in bad faith in its unilateral decisions to (1) close Claimant's OneDrive account, (2) block Claimant from accessing the tens of thousands of files, documents, data, and back-ups that he has stored on OneDrive, and (3) confiscate tens of thousands of Claimant's files, documents, data, and back-ups that were stored on OneDrive and unretrievable in any other format due to Microsoft's faulty Windows update. Microsoft likewise has acted in bad faith in failing to timely and appropriately discuss with Claimant the reason for Microsoft's unilateral actions, as is required under the MSA and principles of law and equity. In addition to the foregoing, additional examples of Microsoft's bad faith are summarized below.

A. In Bad Faith, Microsoft Chose Not to Verify Claimant Actually Shared CSEAI Before Leveling Extreme, False Allegations of Sharing CSEAI

In their Supplement filed May 10, 2021 (the "Recap Admission"), Microsoft admits that the company never actually reviewed any of their files kept in the ordinary course of business to determine whether Claimant actually had shared alleged illegal CSEAI via OneDrive. But this bad faith was not a one-time event, but a recurring one. At each stage of this arbitration, Microsoft and their counsel consistently argued vociferously and without equivocations that they were absolutely certain Claimant had shared illegal CSEAI with third parties. Even during the oral arguments in January 2020 regarding Claimant's Motion for Emergent Relief, counsel for Microsoft highlighted all of the different ways that Claimant could have (and/or did) shared CSEAI via OneDrive. Yet, prior to that oral argument, not a single human within Microsoft took the most basic step (including Mr. Davis who swore under oath and penalty of perjury in the State of New Jersey) to actually review and verify that basic fact with Microsoft's simplest records of Claimant's OneDrive usage.

Exhibit 2 to the Third Amended Claim (submitted March 12, 2021) shows very clearly that Claimant had only "8 items shared" in his entire history of his OneDrive account. Claimant alleges that all of those 8 shared items were shared with himself as he was emailing himself documents to retrieve internet website passwords and credit card numbers. This image was one of only 4 'screens' in Claimant's OneDrive iPhone app. Claimant was able to access this screen

in approximately 30 seconds to verify that he had only shared 8 items in the history of his OneDrive account.

Since Claimant's OneDrive account had been disabled by Microsoft, Claimant could not access the details or the dates of the 8 items shared, but of course Microsoft could have easily accessed those details at any time since the filing of this arbitration in August, 2020 and found that NO items were shared by Claimant on May 12, 2020, let alone illegal CSEAI. There was no need to even examine 'metadata' from any alleged image. In addition, this material 'metadata' was not shared with Claimant's counsel, even though requested in discovery.

B. In Bad Faith, Microsoft Intentionally Delayed Disclosing Their Illegal Scanning of Private Documents in Order to Avoid that Information Becoming Public.

Even AFTER Microsoft was directly presented with the evidence above of the 8 shared items via OneDrive, Microsoft, one of the largest companies, and allegedly 'industry leaders', in the technology world, took 30 full days to discover what a lay claimant was able to discover in 30 seconds. And that was after Microsoft had not looked at any of Claimant's OneDrive sharing information for nearly a year. Microsoft intentionally and in bad faith withheld the information of its faulty recap function that triggered illegal scanning of nearly all of Microsoft's OneDrive's customers. This allegation directly contradicts Microsoft's claim and creates a very serious issue of material fact that "Promptly upon becoming aware that the "recap" feature caused PhotoDNA to scan the image here, Microsoft disclosed these details to Claimant's counsel." (Supplement pages 1-2)

The reason for Microsoft's intentional withholding of information radically affecting the trajectory of these proceedings is simple—Microsoft and their counsel in bad faith illegally manipulated these proceedings in order to wait until the protective order was put into place in this arbitration before revealing the absolute bombshell that Microsoft was illegally invading the privacy of nearly its entire customer base world-wide by scanning private files that were not shared with a third party. Microsoft's customer base would materially shrink overnight if that core fact were released publicly and undoubtedly affect other Microsoft business lines. Behemoth competitors like Amazon, Dropbox, Google and others would immediately take advantage of this key revelation in their marketing to current or would be OneDrive customers that those companies respect their customer's privacy and don't look at their customer's private files. In the context of the massive public policy and media scrutiny of Big Tech firms for their potential privacy intrusions, particularly in the context of expected legislative overhauls of Section 230 in the US and the December 2020 EU ban on the scanning of any OneDrive documents (including those shared), the import of Microsoft's illegal scanning cannot be overstated.

In their own Supplement admitting their illegal scanning and their answers to interrogatories, Microsoft itself demonstrates they intentionally and in bad faith delayed sharing the Recap Admission. First, in their Supplement, Microsoft says they "Recently, however, through investigating Exhibit 2 to the Third Amended Claim, Microsoft discovered that a "recap" feature in OneDrive..." Microsoft admits the trigger to their investigation was precisely caused by Claimant's evidence showing Microsoft's bogus and unverified claims. Second, but prior to notifying Claimant's counsel, "Microsoft has also disabled the [recap] feature" (Supplement page 2). Critical to discovery in this matter, WHEN did Microsoft disable the recap

feature to minimize their loss exposure? How many files did PhotoDNA scan of Claimant's (if all, then all Claimant's files are cleared of CSEAI)? How long has the recap function been in effect? What impact does this illegal scanning of already scanned documents have on the true error rate of PhotoDNA? But, third, and most damning, Microsoft submitted meticulously prepared interrogatory answers late on Wednesday, April 7, 2021, the date the protective order went into effect. Claimant also submitted document and interrogatory responses to Microsoft that same day. Counsel for Microsoft called counsel for Claimant approximately **36 hours later saying that based on Claimant's discovery responses**, Microsoft had determined they had scanned Claimant's private files. But yet in Microsoft interrogatory responses PRIOR to receiving Claimant's discovery responses and PRIOR to the protective order going into place, Microsoft's counsel had plenty of time to ensure that they had correct responses that did NOT allege Claimant had 'shared via OneDrive' CSEAI, but instead merely had an alleged CSEAI stored in his OneDrive account. In Ms. Nahabet's own email to Claimant's counsel on April 12, 2021, "Microsoft's responses to the interrogatory requests were and still are accurate." If Microsoft's counsel had time to prepare in advance and submit meticulously accurate interrogatory responses based on the new information by April 7, 2021, they certainly did not disclose the new information to Claimant's counsel "promptly" on April 9, 2021. The reason is simple—Microsoft in bad faith intentionally delayed disclosure to opposing counsel their egregious lies because they wanted to ensure Claimant was restricted by the protective order not to publicly disclose that same information that would be important to millions of Microsoft's customers, particularly the ones who had been accused of illegally sharing CSEAI via OneDrive and had their OneDrive accounts closed in bad faith.

C. In Bad Faith, Microsoft Alleges that Claimant's 'Activity' Was in Violation of the MSA

Microsoft maintains that Claimant violated the Microsoft Services Agreement (MSA). The MSA's Code of Conduct prohibits users from "engag[ing] in any activity that exploits, harms, or threatens to harm children," or "engag[ing] in activity that violates the privacy of others." (Supplement, page 2) The critical component of that false accusation is that post Recap Admission, Microsoft now does not, nor cannot based on any evidence that they have presented, demonstrate in any fashion that Claimant engaged in any "**activity**" that would violate the MSA. Microsoft alleges without evidence that a single CSEAI was discovered in Claimant's OneDrive account, but Microsoft takes the illogical leap, without any evidence and any diligence on their end, that Claimant had any activity, knowledge, participation or even awareness of any CSEAI image even if such an image exists. Microsoft is fully aware, based on their own expertise as well as Claimant's direct explanations, that images are automatically uploaded to an iPhone user's Photos application from all kinds of other applications on an iPhone. If an image is automatically downloaded to a Photos file that has nearly 7000 images in it, Microsoft cannot allege that a user has engaged in an "activity" that would violate the MSA, which is precisely why Microsoft's policies and procedures are set up to ONLY scan images that are 'shared' because the sharing function is the "activity." Merely being a passive, unknowing and/or unaware recipient of an image is not grounds for any kind of violation. And that assumes there is some of actual CSEAI involved, which is not the case in these circumstances. Here, at most, Claimant was a passive and unknowing recipient of an image that Microsoft flagged as CSEAI.

Claimant did not solicit CSEAI, did not review CSEAI, did not know he had an image in his OneDrive account that qualified as CSEAI, and did not share CSEAI.

Microsoft filed their CyberTipline report at 10:01:56 AM EDT on May 12, 2020 (See Exhibit A to Sean Davis Affidavit). That is the only indication Microsoft has presented in this entire case of when PhotoDNA may have flagged an alleged CSEAI in Claimant's account. In the attached Exhibit A (the reformatted response (reformatted purely for readability from the original) from Verizon to the subpoena Claimant sent them for his SMS and MMS records) and Exhibit B (Claimant's voice cell phone records), all three show Claimant didn't use his cellphone for cell/text communications from 10:22 PM ET on May 11 until 11:41 AM ET on May 12. Moreover, those records show there was no receipt of any images, let alone CSEAI, during that period. Claimant hadn't used his cellphone for a good 12 hours for voice or text messages prior to the time Microsoft reported him to NCMEC for distributing CSEAI. Microsoft produces no evidence whatsoever that Claimant engaged in any "activity" that resulted in even receipt of CSEAI and Claimant has produced every shred of evidence he can find that he wasn't engaged in any "activity" at the 10:01:56 time in question because he was asleep at the time Microsoft alleges he shared, or actively received, an alleged CSEAI. And yet, in bad faith, Microsoft makes more damaging and unsubstantiated allegations that Claimant's nefarious 'activities' are the basis for Microsoft confiscating his tens of thousands of important personal and private documents, data and backups.

But the second part of Microsoft's claim in their Supplemental Answer at the outset of this subsection also goes to their complete bad faith in making scurrilous accusations. First, there has never been any accusation that Claimant has engaged in any "activity that violates the privacy of others." Second, it should be clear from this case that it is Microsoft itself in bad faith who is violating the privacy of others that it appears to hold up as such an important value that it would include it in its MSA.

Lastly, it is essential to highlight that PhotoDNA has scanned all of Claimant's files, and cleared all but allegedly one image. Yet, Microsoft has blocked Claimant from accessing all of his files, and Microsoft has confiscated all of Claimant's files, notwithstanding the fact that, for tens of thousands of files, there is no allegedly objectionable material.

D. In Bad Faith, Microsoft is Willfully Blind to the Faults and Limitations of PhotoDNA

Microsoft's failure to produce the image and failure to name one person who reviewed the flagged image is particularly egregious in light of the company's admission that the PhotoDNA program is prone to error. Microsoft alleges that PhotoDNA has an error rate of 1 in 50 billion scans, based on Dr. Hany Farid's ("Farid") single Congressional testimony. First, Claimant disputes that figure and seeks to engage in discovery to uncover the actual error rate for false positives. Second, Farid's statement in his Congressional testimony is not specific to *false positives*—which is the key metric relevant to Microsoft's bad faith behavior in this matter—but rather refers to errors. In other words, Farid's statement regarding error rates does not adequately capture the number of false hits where PhotoDNA erred in falsely identifying an unobjectionable image as an objectionable one. Third, in his testimony, Farid does not offer the scientific or mathematical basis of his estimate of the error rate. This omission may only be cured with further discovery. Fourth, Farid, a professor at Dartmouth, was one of the key developers of PhotoDNA—

a professor who has staked a significant amount of his professional career and credibility on the efficacy of the PhotoDNA, and someone who benefits financially from the success of PhotoDNA, maintains deep bias and is laden with conflicts of interest. Fifth, even if Farid's analytics was correct when he performed them, it does not follow that the data remain true today since the volume of images has increased significantly and the ability to manipulate images has complicated and compromised the accuracy of scanning algorithms such as PhotoDNA. Sixth, by Microsoft's admission in this arbitration, images stored on OneDrive that were shared already and scanned (and hence cleared as non-CSEAI) were **rescanned** by PhotoDNA as the recap function falsely marked them as shared. This rescanning of images which had already been cleared of CSEAI, massively changes the denominator in the fraction of how many errors PhotoDNA makes. Microsoft has failed to disclose any indication so far as to the extent of that rescanning, and hence the critical need to understand that true denominator of the error rate.

Indeed, even assuming *arguendo* Microsoft's 1 in 50 billion error rate, the frequency of false hits is alarming. Over 3 billion images are shared on the internet each day.⁸ With PhotoDNA, that would translate to a false positive hit approximately twice a month. At one point in this arbitration Microsoft indicated that PhotoDNA scans 1.8 billion images each day. *See* Davis Aff. at 3. Thus, even if all the rosiest projections of PhotoDNA were stipulated at 1 in 50 billion error rate (which Claimant strenuously objects to as a fact), PhotoDNA would falsely identify an image shared via OneDrive every 27.77 days, or approximately at least 13 false positives per year. Alternatively, if PhotoDNA's error rate were 1 in 1.8 billion, PhotoDNA would falsely flag a CSEAI every day of the year.

But in the very limited and inadequate discovery provided by Microsoft, they claim that "in 2020, approximately 13,300 OneDrive accounts worldwide were permanently suspended after PhotoDNA detected at least one match that Microsoft had confirmed as CSEAI...Microsoft is unaware of any instance where a "human rejected PhotoDNA's determination" that an image was a match to an image in the CSEAI database. PhotoDNA does not flag documents, communications, or audio recordings." (Interrogatories, page 6) So even though in Microsoft's rosiest projections, PhotoDNA makes 13 mistakes per year, but Microsoft's alleged human review of every PhotoDNA flag has NEVER rejected PhotoDNA's automated determination. So even with facts Microsoft presents in their absolute best projections, Microsoft knowingly and in bad faith falsely accuse, and report to the NCMEC for federal criminal investigation, on average at least 13 consumers per year of felonies of illegally sharing child pornography AND confiscate those consumers' files. And yet, Microsoft further admits Microsoft intentionally "has not maintained records showing a "rate of PhotoDNA false-positives." (Interrogatories, page 4) This willful ignorance, along with knowingly falsely accusing its own customers of felonious behavior is precisely why Microsoft's policies and procedures are tantamount to bad faith. And without further and appropriate discovery, only this tip of the iceberg will be seen by one Claimant, while countless other OneDrive users will have suffered false accusations and lost access to all of their irreplaceable personal documents, data and backups. Microsoft sums the

⁸ *See* T.J. Thomson, et al., *3.2 Billion Images and 720,000 Hours of Video are Shared Online Daily*, THE CONVERSATION (Nov. 2, 2020). Available at: <https://theconversation.com/3-2-billion-images-and-720-000-hours-of-video-are-shared-online-daily-can-you-sort-real-from-fake-148630>.

effect of Microsoft’s errors succinctly with their Interrogatory Response No. 2 that Microsoft “has not reactivated a OneDrive account that it permanently suspended and closed...” (Interrogatories, page 4)

E. Microsoft’s Bad Faith Conduct Has Cause Significant Harm to Claimant

This case—quite unfortunately for Claimant—is one of the cases where PhotoDNA falsely flagged an image as CSEAI *and* Microsoft failed, in bad faith, to conduct a reasonable human review both as to whether the image had been shared by Claimant and as to whether there is any flagged image that qualifies as CSEAI. This case has sent Claimant diving down rabbit holes, causing immense strain to his personal and professional life. His marriage has suffered immensely as his wife is a child psychologist who works with troubled and challenged adolescents in the New Jersey public school system. Due to Microsoft’s false and damaging accusations that on their face may appear to be credible given Microsoft’s dominance in the technology world, she has had to consider that not only has her husband been collecting child pornography, but that he has been actively sharing that child pornography with others. For Claimant, this case is much more than just the very reasonable need to reclaim access to his private documents and to recoup his extensive out-of-pocket family expenses in prosecuting this matter. This case is also very much about clearing his name of egregious and false accusations set forth and repeated over and over in bad faith by Microsoft without any verification.

IX. Microsoft Violated New Jersey Consumer Protection Laws

Based on the foregoing, which are incorporated herein by reference, Microsoft has violated the New Jersey Consumer Fraud Act, *N.J.S.A. 56:8 et seq.* Specifically, Microsoft has engaged in one or more unconscionable commercial practices, deception, fraud, false pretenses, false promises, and/or misrepresentations that have harmed Claimant. Microsoft also has knowingly concealed, suppressed, and/or omitted material facts in its interactions with Claimant. Accordingly, Claimant is entitled to damages, treble damages, costs, and attorneys’ fees, and may be entitled to statutory damages depending on the nature and extent of Microsoft’s wrongful conduct.

X. The MSA’s Class Action Waiver Should Not be Enforced

Based on the foregoing, which are incorporated herein by reference, Claimant respectfully submits that the class action waiver in the MSA should not be enforced due to Microsoft’s egregious, wrongful, and bad faith conduct. Moreover, the class action waiver in the MSA should not be enforced because Microsoft’s egregious, wrongful, and bad faith conduct extends to conduct not contemplated by the parties when they entered into the agreement. Specifically, the parties did not contemplate that Microsoft would repeatedly scan the private files of Claimant that were not shared via OneDrive. For this portion of Microsoft’s egregious, wrongful, and bad faith conduct, a class remedy is necessary because the harms revealed during

this arbitration reach far beyond Claimant's instance, and implicate the privacy and contractual rights of millions of Microsoft customers. Public policy mandates that Microsoft be held accountable for its egregious conduct, which only can be remedied by remedies that are available to the entire class of individuals who are OneDrive customers.

REQUEST FOR RELIEF

Therefore, Claimant Thomas Deutsch requests that the arbitrator make findings and enter awards as follows:

- 1) That Claimant did not possess or share CSEAI;
- 2) That Microsoft breached the MSA and any enforceable contract with Claimant;
- 3) That Microsoft breached the implied covenant of good faith and fair dealing;
- 4) That Microsoft has been negligent;
- 5) That Microsoft breached the privacy of Claimant;
- 6) That Microsoft committed conversion;
- 7) That Microsoft violated the New Jersey Consumer Fraud Act, *N.J.S.A. 56:8 et seq.*;
- 8) That the MSA's limitation on liability should not be enforced;
- 9) That the MSA's limitation on class actions should not be enforced;
- 10) That Microsoft provide Claimant with full and complete access to all of the contents of his 365 Service;
- 11) That Microsoft reimburse Claimant an additional \$245.23 for Claimant's purchase of Microsoft Office Home & Business 2019 on January 18, 2021 (to replace the Office version destroyed by Microsoft's Defective Windows Update);
- 12) That Claimant be awarded monetary damages to account for Microsoft's acts and omissions, which exceed \$75,000;
- 13) That Claimant be awarded reasonable attorneys' fees and costs;
- 14) That Claimant be awarded punitive or exemplary damages to account for Microsoft's egregious and/or reckless acts and omissions, and/or Microsoft's wanton disregard for Claimant's rights;
- 15) That Claimant be awarded treble damages and/or statutory damages, as may be appropriate; and
- 16) That Claimant be granted such other and additional relief as the arbitrator deems appropriate.

[Signature on Following Page]

Dated: June 8, 2021

SALZANO, LAMPERT & WILSON, LLP

By: /s/ Frank Salzano

Frank Salzano, Esq. (NY SBN 4114849)
275 Madison Avenue, 35th Floor
New York, New York 10016
(646) 863-1883
fsalzano@slwlawoffices.com

Attorneys for Claimant

EXCERPTED EXHIBIT 23

AMERICAN ARBITRATION ASSOCIATION

THOMAS DEUTSCH, ESQ.,

Claimant,

CASE NO. 01-20-0014-3715

v.

MICROSOFT CORPORATION,

Respondent.

**CLAIMAINT'S OPPOSITION TO
RESPONDENT'S MOTION FOR JUDGMENT ON THE PLEADINGS**

TABLE OF CONTENTS

INTRODUCTION	5
ARGUMENT	9
I. Legal Standard	9
A. Motion for Judgment on the Pleadings	9
B. The Limits of Section 230 Immunity	10
II. Section 230 Immunity Does Not Apply to Document Storage Services	12
III. Section 230 Immunity Does Not Apply Because Microsoft Scanned and Confiscated All of Claimant's Private Files Without His Consent	18
IV. The Motion Should Be Denied Because Several Material Issues of Fact are Disputed	21
A. There is a Material Dispute of Fact As to Whether There is Any Image that Qualifies as CSEAI	22
B. There is a Material Dispute of Fact As to Whether Microsoft Conducted Human Review of the Flagged Image	25
C. There is a Material Dispute of Fact As to Whether Microsoft Maintained Subjective Good Faith	26
V. The MJOP Does Not Seek to Dismiss All Claims in this Arbitration	30
VI. Insofar as the Motion Is Granted Due to a Pleading Deficiency, Claimant Respectfully Requests Leave to Amend the Pleadings	31
CONCLUSION	32

TABLE OF AUTHORITIES

CASES

<i>AirBnB, Inc. v. City of Boston</i> , 386 F. Supp. 3d 113, 119-121 (D. Mass. 2019).....	17
<i>Bennett v. Google, LLC</i> , 882 F.3d 1163, 1164-1168 (D.C. Cir. 2018)	17
<i>Domen v. Vimeo</i> , 991 F.3d 66, 68 (2d Cir. 2021).....	13
<i>Enhanced Athlete Inc. v. Google LLC</i> , No. 19-CV-08260-HSG, 2020 WL 4732209 at *1 (N.D. Cal. Aug. 14, 2020)	17
<i>Enigma Software Grp. USA, LLC v. Malwarebytes, Inc.</i> , 946 F.3d 1040, 1047 (9th Cir. 2019), <i>cert. denied</i> , 141 S. Ct. 13 (2020)	29
<i>Fair Housing Council of San Fernando Valley v. Roommates.Com, LLC</i> , 521 F.3d 1157, 1163-1164 (9th Cir. 2008)	10
<i>Federal Agency of News LLC v. Facebook, Inc.</i> , 432 F. Supp. 3d 1107, 1112-1113 (N.D. Cal. 2020).....	14
<i>Franklin v. X Gear 101, LLC</i> , 2018 WL 4103492, at *1 (S.D.N.Y. Aug. 28, 2018).....	15
<i>Green v. America Online (AOL)</i> , 318 F.3d 465, 468-470 (3d Cir. 2003)	15
<i>Hansen v. Hansen</i> , 770 A.2d 1278, 1286 (N.J. App. Div. 2001)	31
<i>Holomaxx Technologies v. Microsoft Corp.</i> , 783 F. Supp. 2d 1097, 1101-1102 (N.D. Cal. 2011)	16
<i>International Raw Materials, Ltd. v. Stauffer Chem. Co.</i> , 978 F.2d 1318, 1327 n. 11 (3d Cir.1992).....	31
<i>Kernan v. One Washington Park</i> , 154 N.J. 437, 456–57 (N.J. 1998)	31
<i>Kolebuck-Utz v. Whitepages Inc.</i> , No. C21-0053-JCC, 2021 WL 1575219, at *3 (W.D. Wash. Apr. 22, 2021).....	21
<i>Massachusetts Port Auth. v. Turo Inc.</i> , 487 Mass. 235, 241–42, 166 N.E.3d 972, 980 (2021)	12
<i>Nieman v. Versuslaw, Inc.</i> , 2012 WL 3201935, at *4 (C.D. Ill. 2012)	16
<i>Obado v. Magedson</i> , 612 Fed. App’x 90, 92 (3d Cir. 2015).....	15
<i>Page v. Oath Inc.</i> , No. CV S20C-07-030 CAK, 2021 WL 528472, at *7 (Del. Super. Ct. Feb. 11, 2021).....	17

<i>Poole v. Tumblr, Inc.</i> , 404 F. Supp. 3d 637, 639-640 (D. Conn. 2019)	15
<i>Putt v. TripAdvisor Inc.</i> , No. CV 20-3836, 2021 WL 242470, at *4 (E.D. Pa. Jan. 25, 2021)	21
<i>Riggs v. MySpace, Inc.</i> , 444 Fed. App'x. 986, 987-988 (9th Cir. 2011)	15
<i>Smith v. Trusted Universal Standards in Electronic Transactions, Inc.</i> , 2011 WL 900096, at *1-3 (D.N.J. Mar. 15, 2011).....	14, 16
<i>Song fi Inc. v. Google, Inc.</i> , 108 F. Supp. 3d 876, 884 (N.D. Cal. 2015).....	29
<i>Stratton Oakmont, Inc. v. Prodigy Services Co</i> , No. 31063/94, 1995 WL 323710, at *1 (N.Y. Sup. Ct. May 24, 1995).....	9
<i>Syncsort Inc. v. Sequential Software, Inc.</i> , 50 F. Supp. 2d 318, 324 (D.N.J. 1999).....	passim
<i>Wolfington v. Reconstructive Orthopaedic Associates</i> , 935 F.3d 187, 195 (3d Cir. 2019)....	passim
<i>Zango, Inc. v. Kaspersky Lab, Inc.</i> , 568 F.3d 1169, 1178-80 (9th Cir. 2009).....	29
<i>Zimmerman v. Corbett</i> , 873 F.3d 414, 417-418 (3d Cir. 2017).....	9, 19

STATUTES

47 U.S.C. § 230(c)	6, 10, 12, 18
--------------------------	---------------

INTRODUCTION

Claimant Thomas Deutsch (hereinafter “Claimant”) brings this consumer arbitration because Respondent Microsoft Corporation (hereinafter “Microsoft” or “Respondent”) wrongfully closed Claimant’s OneDrive account, Microsoft wrongfully precluded Claimant from accessing his files stored on OneDrive, and Microsoft wrongfully confiscated thousands of Claimant’s documents that are stored on OneDrive. At the outset of this case and for nearly a year thereafter, Microsoft asserted that the sole reason for its conduct is that Microsoft’s computer program, PhotoDNA, allegedly flagged a single image that Claimant allegedly shared via OneDrive that Microsoft asserts is child pornography. *See* Microsoft’s Answer to Claimant’s Demand for Arbitration and Defenses at 1; *see also* Microsoft’s Answer and Defenses to Claimant’s Third Amended Claim at 1. This alleged image, which Microsoft blindly asserts as illegal child sexual exploitation and abuse imagery (hereinafter “CSEAI”), has not been reviewed by any named individual within Microsoft, has not been reviewed by counsel for Microsoft, has not been independently verified as CSEAI by any third party, has not been shared with the Arbitrator in this matter, and has not been produced to Claimant or Claimant’s counsel.

After discovery began in this matter, Microsoft made several material admissions that altered the trajectory of this matter and revealed the tip of the iceberg regarding Microsoft’s bad faith and wrongful conduct. First, Microsoft admitted that one of its officers included false statements in a written and signed affidavit provided to this forum. *See* Microsoft’s Supplement to its Answer to Claimant’s Third Amended Claim (“Supplement”), ¶ 1-5; *see also* Affidavit of Sean Davis in Support of Microsoft’s Opposition to Motion Seeking Emergent Relief (“Davis Aff.”), ¶ 9. Second, contrary to its repeated affirmations that spanned nearly twelve months, Microsoft admitted that the company scanned Claimant’s private documents beyond that permitted by the

Microsoft Services Agreement (hereinafter “MSA”), Microsoft’s Privacy Statement (hereinafter “Privacy Statement”), and that detailed by Sean Davis (hereinafter, “Davis”), Microsoft’s Head of Digital Safety Operations. *See id.*; *see also* Exhibit A to Supplement, Privacy Statement; *see also* Exhibit A to Davis Aff., MSA. Third, Microsoft further admitted that it was incorrect in asserting that Claimant shared alleged CSEAI via OneDrive or any other means. *See* Supplement, ¶ 1-5.

Throughout this arbitration, Microsoft has gone to great lengths to highlight one essential point: the MSA grants Microsoft the authority to scan files that Claimant shares via OneDrive but does not give Microsoft the right to scan Claimant’s private files that are simply stored on OneDrive. *See* Davis Aff., ¶ 9; *see generally* MSA; Privacy Statement. Specifically, Davis affirmed in his signed affidavit:

“To balance the privacy of its customers against the company’s legitimate business interest in ensuring safe services, Microsoft runs PhotoDNA only when images are shared or made public from a customer account; Microsoft does not search its customers’ private files. That is, customer accounts remain private; it is only when data is shared by a customer that PhotoDNA becomes operative.”

Davis Aff., ¶ 9.

Microsoft’s very specific policies and procedures for scanning private documents is not coincidental. Rather, Microsoft crafted its policies and procedures specifically to parallel Section 230 of the Communications Decency Act of 1996 (“CDA”), which only grants a safe harbor in instances where an interactive service provider restricts access to objectionable matter that is shared with a third party. *See* 47 U.S.C. § 230(c); *see also infra* Sections I(B), II, and III.

Microsoft attempted to downplay its egregious and unlawful conduct—which also constitutes a breach of contract and invasion of privacy—by deeming it a mere oversight. *See* Supplement, ¶ 1-5. Yet, it defies logic and common sense for Microsoft—one of the largest technology companies in the world—to contend that the company unknowingly was scanning

billions of its customers private files per week because of an “oversight” in its OneDrive recap function. Indeed, Microsoft’s “oversight” would not have come to light had discovery not commenced in this matter.

More to the point for this motion, Microsoft’s scanning of Claimant’s private documents—which were not shared with anyone—places Microsoft’s illegal and bad faith conduct outside the bounds of Section 230. That is, even if the MSA allows Microsoft the ability to scan private files (which it does not), Section 230 immunity does not protect Microsoft should it engage in wrongful or bad faith conduct during such scans of private documents or in connection with Microsoft’s negligent or otherwise wrongful actions and omissions thereafter.

Within days of Microsoft’s admissions of wrongful conduct, Microsoft sought for and obtained a stay of discovery so that the parties could explore settlement of this matter. Settlement discussions stalled, at which point Microsoft sought and obtained the right to file a motion for judgment on the pleadings that the Arbitrator would consider contemporaneously with Claimant’s pending motion to compel. Microsoft’s motion for judgment on the pleadings (“MJOP”) is based on one legal claim, that the company maintains immunity from suit under Section 230 of the CDA.

Previously, the parties agreed that Microsoft would file its Section 230 motion after the close of discovery. *See* Scheduling Order No. 1. This was because the legal issue of Section 230 immunity directly hinges on several factual elements that would be revealed during discovery. Despite the earlier agreement between the parties regarding the timing of Microsoft’s Section 230 motion—and only after Microsoft admitted that it breached the MSA and illegally scanned Claimant’s private documents—Microsoft sought for and obtained permission to file its Section 230 motion prior to the close of discovery and sought for and obtained a stay of discovery pending resolution of Claimant’s motion to compel and the MJOP.

Microsoft dubiously contends that Section 230 of the CDA bars Claimant from any redress, (1) regardless of whether Microsoft wrongfully closed Claimant's OneDrive account, (2) regardless of whether Microsoft wrongfully precluded Claimant from accessing his files stored on OneDrive, (3) regardless of whether Microsoft wrongfully confiscated thousands of Claimant's documents that are stored on OneDrive, (4) regardless of whether Microsoft illegally scanned Claimant's private documents, (5) regardless of whether Microsoft admitted that it breached the terms of the MSA; (6) regardless of whether Claimant actually had CSEAI in his OneDrive account, and (7) regardless of the fact that Claimant did not share any objectionable material via OneDrive or otherwise. Microsoft grossly mischaracterizes the bounds of the legal immunities afforded by Section 230 in a brazen attempt to radically expand the scope of those immunities and evade responsibility for its widespread and far-reaching illegal and bad faith conduct.

Claimant respectfully submits that the Arbitrator should deny Microsoft's motion. There are four key points. First, Section 230 immunity is limited, and does not apply to fee-for-service document storage services such as Microsoft's OneDrive, particularly for private consumer accounts whose contents are not shared with any third party or made public. Second, even if Section 230 immunity would apply to document storage services, it does not apply in this instance because Microsoft scanned Claimant's *private* files that were *not shared* with a third party. Third, even assuming *arguendo* that Microsoft's PhotoDNA accurately flagged a single image in Claimant's OneDrive account to be objectionable, Section 230 does not immunize Microsoft from confiscating *all* of Claimant's tens of thousands of private files. Rather, the terms of the statute only provide immunity to Microsoft—at most—insofar as Microsoft took efforts to restrict Claimant from accessing and sharing the one allegedly objectionable image. Fourth, the motion should be denied because there are several material issues of fact that are in dispute. For example,

(1) there is a material dispute of fact as to whether there exists any image that PhotoDNA flagged as CSEAI, (2) there is a material dispute of fact as to whether Microsoft conducted human review of the alleged image (as it was required to do under the terms of the MSA), and (3) there is a material dispute of fact as to whether Microsoft maintained subjective good faith in scanning Claimant's private files, closing his account, and confiscating tens of thousands of his documents.

For the reasons outlined herein, Claimant respectfully requests that the Arbitrator deny Microsoft's MJOP.

ARGUMENT

I. Legal Standard

A. Motion for Judgment on the Pleadings

In a motion for judgment on the pleadings, the Arbitrator must "view the facts presented in the pleadings and the inferences to be drawn therefrom in the light most favorable to the nonmoving party." *Wolfington v. Reconstructive Orthopaedic Associates*, 935 F.3d 187, 195 (3d Cir. 2019) (citation omitted). All of the facts outlined in the claim are to be accepted as true, *Zimmerman v. Corbett*, 873 F.3d 414, 417-418 (3d Cir. 2017), and the arbitrator may not grant the motion "unless the movant clearly establishes that no material issue of fact remains." *Wolfington*, 935 F.3d at 195 (citation omitted). Accordingly, for this motion, all facts must be construed in Claimant's favor, and the facts alleged in the claim must be presumed to be true.

A motion for judgment on the pleadings can be granted "only if no relief could be granted under any set of facts that could be proved." *Syncsort Inc. v. Sequential Software, Inc.*, 50 F. Supp. 2d 318, 324 (D.N.J. 1999) (citations omitted). A claim should not be dismissed unless it appears beyond doubt that "the facts alleged in the complaint, even if true, fail to support the claim." *Id.* at

325 (citations omitted). As New Jersey courts explain, in reviewing the sufficiency of a claim on a motion for judgment on the pleadings, a court or arbitrator has a limited role: “The issue is not whether a plaintiff will ultimately prevail but whether the claimant is entitled to offer evidence to support his [or her] claims.” *Id.*

B. The Limits of Section 230 Immunity

The enactment of legal shields in Section 230 was prompted by a state court case, *Stratton Oakmont, Inc. v. Prodigy Services Co.*, that held an internet company that hosted a message board to be responsible for content posted by a user of that message board. *See Stratton Oakmont, Inc. v. Prodigy Services Co.*, No. 31063/94, 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995). Under the court’s rationale, online service providers that voluntarily filtered some messages would be liable for all messages transmitted, “whereas providers that bury their heads in the sand and ignore problematic posts altogether escape liability.” *Fair Housing Council of San Fernando Valley v. Roommates.Com, LLC*, 521 F.3d 1157, 1163-1164 (9th Cir. 2008) (outlining the history of Section 230). As the Ninth Circuit explained, in enacting Section 230, “Congress sought to spare interactive computer services this grim choice by allowing them to perform some editing on user-generated content without thereby becoming liable for all defamatory or otherwise unlawful messages that they didn’t edit or delete. In other words, Congress sought to immunize the *removal* of user-generated content.” *Id.* (emphasis in the original).

Section 230 was not enacted as a catch-all immunity provision for Big Tech companies like Microsoft. Nor was Section 230 immunity enacted to protect document storage systems like OneDrive. Rather, Section 230 immunity was specifically created to allow some tech companies flexibility to police content *shared with other users via interactive services*. *See, e.g., id.* By the

nomenclature of its own enacting legislation, Section 230 is precisely focused on content that is “communicated.”

In line with the limited purpose underlying Section 230 immunity, the legal shields afforded by Section 230 are narrowly tailored to interactive online functions. This is why the statute permits immunity only for companies that offer an “interactive computer service.” 47 U.S.C. § 230(c). Moreover, this is why Davis, Microsoft’s Head of Digital Safety Operations, stated in his sworn affidavit that Microsoft scans documents “only when images are *shared or made public* from a customer account.” Davis Aff., ¶ 9 (emphasis added).

In other words, Microsoft crafted its policies and procedures precisely in an attempt to parallel the legal immunities afforded by Section 230—which are strictly limited to documents or images that, as Microsoft itself explains, “*are shared or made public from a customer account.*” *Id.* (emphasis added).

The parallels between Microsoft’s policies and procedures of only scanning *shared* documents and Section 230 immunity mandates close inspection. Even if, as Microsoft contends in the MJOP, the company had a right to scan Claimant’s private files under the terms of the MSA (which they did not), it does not follow that Section 230 provides immunity for Microsoft’s conduct. *See* MJOP, at 13.

In other words, Section 230 immunity only applies to actions taken by an interactive service provider where the provider seeks to remove information that was *shared* with third parties. This is precisely why Microsoft argued so vigorously and in bad faith—for twelve months—that Claimant shared CSEAI via OneDrive, even though not a single person in all of Microsoft or their counsel went back to verify their automated flagging system was operating correctly. This is also why Microsoft asserted—again for twelve months—that it only scans images that are *shared* via

OneDrive. If Claimant did not share an objectionable image with a third party, then Section 230 immunity does not shield Microsoft's conduct.

Under the terms of the CDA, any scanning of private files that are *not shared* with a third party catapults Microsoft outside the walls of the protections of Section 230. And, once Microsoft is outside the walls of Section 230, it cannot benefit from the statute's legal shields in cases—as in Claimant's instance—where the company has engaged in bad faith conduct by wrongfully closing a user's account and wrongfully confiscating tens of thousands of his private documents that have already been scanned and cleared of CSEAI. *See* Supplement, ¶ 1-5.

To our knowledge and based on what Microsoft presented in its MJOP, no court has ever granted immunity under Section 230 for confiscation of a user's private documents that were in fee-for-service online storage and not shared via any interactive service. Indeed, Microsoft has not cited to a single case that involves a document storage system, or OneDrive in particular, nor has Microsoft cited to a single case that involves confiscation of a user's private documents that were not shared with other users of an interactive system (and had already been scanned and cleared of CSEAI). Rather, Microsoft seeks to bury its wrongful conduct by asking this forum to assert a radical expansion of Section 230 immunity far beyond that envisioned by Congress and far beyond what any court has held to date. Particularly without the benefit of full and fair discovery to plumb the extreme depths of Microsoft's bad faith conduct and policies, this radical expansion of Section 230 immunity should be rejected.

II. Section 230 Immunity Does Not Apply to Document Storage Services

Despite relying on a significant number of cases in its motion papers, Microsoft does not cite to one single case where Section 230 immunity was held to apply to document storage services. This omission is telling and revealing. As detailed in the previous section, the legal shields afforded

by Section 230 were enacted to protect “interactive service providers” who moderate content that users *share with other users* in online and interactive forums. 47 U.S.C. § 230(c). Typical examples of such conduct include sharing an excessively violent video on YouTube, sharing a lewd photo via Twitter, or sharing a lascivious comment on an online message board.

Section 230 immunity was not created to provide immunity for alleged (but wholly unsubstantiated) wrongful conduct regarding fee-paying, online document storage services like OneDrive, nor has any court expanded Section 230 immunity to cover such services. As courts have explained, Section 230 immunity applies solely to instances where “the cause of action necessarily requires that the defendant be treated as the publisher or speaker of content provided by another.” *Massachusetts Port Auth. v. Turo Inc.*, 487 Mass. 235, 241–42, 166 N.E.3d 972, 980 (2021) (citing *Jane Doe No. 1 v. Backpage.com, LLC*, 817 F.3d 12, 16 (1st Cir. 2016), *cert denied*, 137 S. Ct. 622 (2017)). Indeed, it would be a radical expansion of Section 230 immunity to allow Microsoft full legal cover for its admittedly wrongful conduct in this matter, which involves the scanning of Claimant’s private documents that were merely automatically stored on Microsoft’s OneDrive document storage system, and then Microsoft’s confiscation of tens of thousands of his private files that have already been scanned and cleared of containing CSEAI. *See* Supplement, ¶ 5.

A review of the cases upon which Microsoft relies underscores the limited reach of Section 230 immunity and the radical expansion proposed by Microsoft in its MJOP. For example, the *Vimeo* decision from the Second Circuit involves Vimeo, a web-based, video-sharing platform. *Domen v. Vimeo*, 991 F.3d 66, 68 (2d Cir. 2021). The defendant in that case, Vimeo, deleted plaintiff’s account because plaintiff shared videos publicly that expressed views that discriminated against individuals based on their sexual orientation. *See id.* at 68-70. Vimeo removed the videos—

which were available to other users of Vimeo—from the online forum and closed plaintiff’s account. *See id.* But prior to removing the videos and closing the account, Vimeo warned the plaintiff about sharing objectionable content and gave the plaintiff an opportunity to cease its objectionable conduct. *See id.* at 69. The plaintiff chose to ignore Vimeo’s warning and continued to share objectionable content publicly. *See id.* at 73. In Claimant’s instance, and pursuant to specific Microsoft policies and procedures, Claimant not only did not receive any kind of warning that he had a single alleged objectionable image in his private OneDrive storage, Microsoft did not even notify Claimant why his tens of thousands of important documents had been confiscated. Although the *Vimeo* court upheld immunity based on Section 230, it did so only because the gravamen of the suit involved taking down *offensive content that was intentionally shared in an online public forum*. *See id.* Nothing in the case involved Vimeo examining the *private* files of the plaintiff in that case.

In *Vimeo* and every other case that Microsoft cites, the objectionable content was publicly available for the court to review, and the court verified that the content existed and was subjectively offensive. In Claimant’s matter, there is material dispute of fact as to whether any image exists that Microsoft could find objectionable, save for the unreliable affidavit of Davis that Microsoft has already admitted was materially false and produced without Davis actually verifying for himself that Claimant shared any images whatsoever via OneDrive (let alone Davis verifying himself that the shared image was in fact CSEAI).

Further, none of the cases cited by Microsoft involve a document storage system whereby a consumer specifically entered into a contract and paid a fee, so that the consumer could back-up and protect their files from loss. Here, the precise reason for the contract and paid fee was to protect

Claimant's files from loss—which has been the very outcome of Microsoft's confiscation and faulty Windows update program. *See* Claimant's Fourth Amended Claim at 8.

A close review of the cases that Microsoft cites in its MJOP illustrates these points. *See* MJOP, at 5-6 In *Smith*, the defendant Microsoft blocked email communications that were intentionally sent and shared by the plaintiff to other users. *Smith v. Trusted Universal Standards in Electronic Transactions, Inc.*, 2011 WL 900096, at *1-3 (D.N.J. Mar. 15, 2011). The court in *Smith* did not extend Section 230 immunity to cover Microsoft's review of plaintiff's private files. The *Facebook* case involved Facebook closing an account and taking down content posted by a Russian group that **shared** and posted information publicly to meddle in the 2016 U.S. presidential election. *Federal Agency of News LLC v. Facebook, Inc.*, 432 F. Supp. 3d 1107, 1112-1113 (N.D. Cal. 2020). Nothing in the *Facebook* case related to the scanning of private and unshared files. In *Riggs*, the defendant MySpace deleted the user's profile on a public social networking platform after the user **shared** comments on the platform. *Riggs v. MySpace, Inc.*, 444 Fed. App'x. 986, 987-988 (9th Cir. 2011). *Riggs* likewise did not involve a defendant that scanned a plaintiff's private files. *Poole* involved a case where plaintiff alleged that defendant Tumblr—an interactive web platform that allows users to publicly post photographs, videos, music, and comments—illegally allowed a third-party user to publicly **share** photos of her and failed to take reasonable efforts to delete the photographs that were shared publicly without consent. *Poole v. Tumblr, Inc.*, 404 F. Supp. 3d 637, 639-640 (D. Conn. 2019). The case did not involve defendant Tumblr scanning the private files of a user on its platform. And, in *Franklin*, the case involved copyright and trademark infringement after a user **shared** publicly allegedly infringing images of a logo. *Franklin v. X Gear 101, LLC*, 2018 WL 4103492, at *1 (S.D.N.Y. Aug. 28, 2018). Again, the case did not involve the scanning of private files of a user of a document storage service. The *Green*

case dealt with alleged *sharing* of defamatory statements in an internet chat room and did not involve scanning of private unshared files of a user of a document storage system. *Green v. America Online (AOL)*, 318 F.3d 465, 468-470 (3d Cir. 2003). The *Obado* case likewise involved alleged *sharing* of defamatory statements and did not involve scanning of private files of a user of a document storage system. *Obado v. Magedson*, 612 Fed. App'x 90, 92 (3d Cir. 2015).

Microsoft further engages in bad faith conduct by providing disingenuous and deceiving citations when it alleges that the company's fee-for-service OneDrive product qualifies as an "interactive service" under the terms of Section 230. *See* MJOP, at 10-11. Microsoft is a massive corporation that offers many products and services. Although some of its products and services may qualify as an "interactive service," Microsoft's OneDrive product does not, particularly for consumer accounts whose contents are not shared at all. For example, if Microsoft operated a physical storage facility and confiscated all the belongings from a consumer's private storage unit because the company allegedly found one objectionable photograph in the private storage room, Microsoft would certainly not be able to claim immunity under Section 230 of the CDA simply because other aspects of Microsoft's business may qualify as an interactive service; this is especially true where, as here, the allegedly objectionable photograph has not been verified by a third party, court, or law enforcement agency as CSEAI. In other words, Section 230 immunity can only apply to how an entity is operating in the legal controversy in question, not whether the entity operates some other functions that could qualify for immunity under the CDA.

The cases Microsoft cites in its brief precisely illustrate this critical distinction. *See* MJOP, at 10-11. In *Holomaxx Technologies*, at issue was Microsoft's email system, not OneDrive. *Holomaxx Technologies v. Microsoft Corp.*, 783 F. Supp. 2d 1097, 1101-1102 (N.D. Cal. 2011). The *Smith* case also dealt with Microsoft's email system, not OneDrive. *Smith*, 2011 WL 900096,

at *1-3. And, in *Nieman*, at issue was Microsoft’s internet search engine, not OneDrive. *Nieman v. Versuslaw, Inc.*, 2012 WL 3201935, at *4 (C.D. Ill. 2012). Indeed, even the definition of “interactive service provider” provided by Microsoft in its own motion papers belies Microsoft’s argument that its OneDrive document storage service qualifies. Specifically, the definition cited by Microsoft states that “internet service providers, website exchange systems, online message boards, and search engines fall within this definition.” MJOP, at 10 (citing *LeadClick*, 838 F.3d at 174). Document storage services are not included on the list. To summarize, not one citation provided by Microsoft has held that its OneDrive product—or any other document storage system—qualifies as an “interactive service provider” for purposes of Section 230 of the CDA.

Apart from the long list of disingenuous citations proffered by Microsoft in its MJOP, several cases that Microsoft omits from its brief underscore the limited reach of Section 230 immunity and why the doctrine does not apply to this matter. For example, in *AirBnB, Inc. v. City of Boston*, the court held that Section 230 immunity did not apply because the defendant was not a publisher or speaker of content shared by any third party. *AirBnB, Inc. v. City of Boston*, 386 F. Supp. 3d. 113, 119-121 (D. Mass. 2019). In *Enhanced Athlete*, defendant Google benefited from Section 230 immunity only insofar as Google removed videos that plaintiff ***shared*** publicly via YouTube and closed plaintiff’s YouTube account because plaintiff used the videos to illegally market medical products that were not FDA-approved for human consumption. *Enhanced Athlete Inc. v. Google LLC*, No. 19-CV-08260-HSG, 2020 WL 4732209 at *1 (N.D. Cal. Aug. 14, 2020). The case did not involve Google terminating an account due to objectionable content found in the plaintiff’s private files that were not shared with a third party. Similarly, *Bennett* involved a claim whereby defendant Google failed to remove videos ***posted and shared*** publicly via YouTube that were allegedly defamatory; the court did not extend Section 230 to the scanning of private files

that were not shared with a third party. *Bennett v. Google, LLC*, 882 F.3d 1163, 1164-1168 (D.C. Cir. 2018). And, in *Page*, the court again affirmed the well-established doctrine that Section 230 immunity applies solely in instances where a defendant takes steps to remove objectionable content “posted” in an interactive public forum and thus shared with a third party. *Page v. Oath Inc.*, No. CV S20C-07-030 CAK, 2021 WL 528472, at *7 (Del. Super. Ct. Feb. 11, 2021).

As a very long line of cases across the country makes clear, for Section 230 immunity to apply, a plaintiff must have shared, posted, disseminated, or otherwise communicated objectionable content with a third party. In this case, Claimant did none of these.

The pattern here is clear: Section 230 immunity does not apply to document storage services and does not apply to instances where a defendant improperly and illegally scans a plaintiff’s *private* files in a document storage system that are *not shared* with any third party.

III. Section 230 Immunity Does Not Apply Because Microsoft Scanned and Confiscated All of Claimant’s Private Files Without His Consent

Microsoft does not cite to one case where Section 230 immunity was extended to cover instances where a defendant improperly scanned and confiscated the private files of a user who did not actively or intentionally share those files with a third party. Moreover, for the first twelve months of this arbitration, Microsoft consistently affirmed that it has never, and would never, scan the private files of its users. *See Davis Aff.*, ¶ 9; Supplement, ¶ 1-5. As Davis affirmed: “Microsoft does not search its customers’ private files. That is, customer accounts remain private; it is only when data is *shared* by a customer that PhotoDNA becomes operative.” *Davis Aff.*, ¶ 9 (emphasis added).

In Claimant’s instance and for what appears to be nearly all of its other customers around the globe, Microsoft violated its own policies and procedures. Specifically, Microsoft admitted to

scanning Claimant's private files that were not shared via OneDrive. *See* Supplement, ¶ 1-5. As detailed in Section II *supra*, Microsoft has not cited to one case where a court found such illegal and bad faith conduct to fall under Section 230 immunity.

Furthermore, by the express terms of the statute, Section 230 of the CDA only grants Microsoft the ability "to restrict access to or availability *of material* that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable." 47 U.S.C. § 230(c) (emphasis added). The statute does not afford tech companies carte blanche to confiscate tens of thousands of documents or materials that do not fit this description. Thus, assuming *arguendo* that Microsoft's PhotoDNA accurately deemed one image in Claimant's OneDrive account to be objectionable, Section 230 does not provide Microsoft immunity to confiscate tens of thousands of Claimant's files, unless Microsoft made a reasonable determination that each and every file is objectionable. In other words, the statute mandates that a company only can "restrict access to" objectionable material. 47 U.S.C. § 230(c).

Here, Microsoft had been scanning all of Claimant's files because its faulty recap function was marking some or even all of Claimant's documents as "shared," which triggered PhotoDNA to scan and clear every image in Claimant's OneDrive account regardless of whether the image actually was shared. *See* Supplement, ¶ 1-5. In Microsoft's admissions in their Supplemental Answer, they do not provide any details as to how long the recap function has been in place and/or how many of Claimant's images were illegally scanned. Based on what Microsoft has disclosed, it appears that all of Claimant's files and images were scanned by PhotoDNA, regardless of whether Claimant shared the files or images.

Here, however, Microsoft confiscated tens of thousands of Claimant's documents based on an illegal scan of his private files. Microsoft alleges that the scan revealed one single image that

allegedly qualifies as CSEAI, yet Microsoft has not produced the allegedly objectionable image. Moreover, counsel for Microsoft has not reviewed the image, the Arbitrator has not reviewed the image, and Microsoft admitted (in its interrogatory responses) that it cannot name even one person who actually conducted a human review of the flagged image. *See* Respondent Microsoft Corporation's Objections and Responses to Claimant's First Set of Interrogatories, at 2-3 (a copy is attached hereto as Exhibit A). This last failure—Microsoft's inability to name one person who conducted a review of the image flagged by its computer program—is in and of itself a violation of Microsoft's own policies and that of the MSA. Moreover, for this motion for judgment on the pleadings, the factual allegations in the claim must be presumed to be true, and all inferences are to be drawn in the light most favorable to Claimant. *See Wolfington*, 935 F.3d at 195; *Zimmerman*, 873 F.3d at 417-418. Thus, as Claimant details in his claim, it must be presumed that there is no CSEAI, and that Microsoft closed Claimant's account and confiscated all his documents without actually finding an objectionable image. *See* Fourth Amended Claim at 5, 16-17.

This case—quite unfortunately for Claimant—is one of the cases where PhotoDNA falsely flagged an image as CSEAI *and* Microsoft failed, in bad faith, to conduct a reasonable human review both as to whether the image had been shared by Claimant and as to whether there is any flagged image that qualifies as CSEAI. *See* Fourth Amended Claim at 19-21. This case has sent Claimant diving down rabbit holes, causing immense strain to his personal and professional life. *See id.* at 21. His marriage has suffered immensely as his wife is a child psychologist who works with troubled and challenged adolescents in the New Jersey public school system. *See id.* Due to Microsoft's false and damaging accusations that on their face may appear to be credible given Microsoft's dominance in the technology world, she has had to consider that not only has her husband been collecting child pornography, but that he has been actively sharing that child

pornography with others. *See id.* For Claimant, this case is much more than just the very reasonable need to reclaim access to his private documents and to recoup his extensive out-of-pocket expenses in prosecuting this matter. *See id.* This case is also very much about clearing his name of egregious and false accusations set forth and repeated over and over in bad faith by Microsoft without any verification or substantiation. *See id.*

One straightforward example illustrates: had Claimant not brought his demand for arbitration to this point of the proceedings, Claimant would have let lie Microsoft's outrageous (and now admittedly false) allegation that Claimant shared CSEAI with a third party. To grant this motion and deny Claimant full and fair evidentiary discovery is tantamount to denying Claimant the proper opportunity to clear his name of the bad faith false accusations by Microsoft. That denial would be well beyond the scope Congress could have ever intended of Section 230 immunity.

Taken together, Claimant respectfully submits that Section 230 immunity does not apply in this matter because Microsoft scanned Claimant's private files that were not shared with a third party, and because Microsoft confiscated thousands of Claimant's files that had no objectionable content in direct violation of the clear terms of Section 230 of the CDA.

IV. The Motion Should Be Denied Because Several Material Issues of Fact are Disputed

It is axiomatic that a motion for judgment on the pleadings must be denied if material issues of fact are disputed. *Wolfington*, 935 F.3d at 195. As courts have made clear, this fundamental principle applies to cases where Section 230 is raised as a defense. *See, e.g., Kolebuck-Utz v. Whitepages Inc.*, No. C21-0053-JCC, 2021 WL 1575219, at *3 (W.D. Wash. Apr. 22, 2021) (denying motion to dismiss on grounds of Section 230 immunity due to dispute of material factual issue); *Putt v. TripAdvisor Inc.*, No. CV 20-3836, 2021 WL 242470, at *4 (E.D. Pa. Jan. 25, 2021) (same).

In this matter, at least three material issues of fact are in dispute: (1) there is a material dispute of fact as to whether there is any image that qualifies as CSEAI; (2) there is a material dispute of fact as to whether Microsoft conducted human review of the flagged image; and (3) there is a material dispute of fact as to whether Microsoft maintained subjective good faith in scanning Claimant's private files, closing his account, and confiscating tens of thousands of his documents.

A. There is a Material Dispute of Fact as to Whether There is Any Image that Qualifies as CSEAI

From the outset of this arbitration Claimant has denied possessing or sharing CSEAI. *See* Claimant's Amended Claim; *see also* Claimant's Second Amended Claim; Third Amended Claim; and Fourth Amended Claim. Moreover, Microsoft has failed to produce any image in this matter. Indeed, no court, law enforcement agency, or independent third party has determined that any image in Claimant's OneDrive account is child pornography. And, a review of Claimant's phone and text records, received from a subpoena to Verizon (his mobile phone carrier), reveal that Claimant did not use his phone for calls or texting during the time period where Microsoft alleges that Claimant shared CSEAI. *See* Fourth Amended Claim at 19. Simply stated, there is nothing in the record to demonstrate that any image is CSEAI. On a motion for judgment on the pleadings, the Arbitrator must "view the facts presented in the pleadings and the inferences to be drawn therefrom in the light most favorable to the nonmoving party." *Wolfington*, 935 F.3d at 195. Thus, for this motion it must be presumed that there is no CSEAI, and that Microsoft closed Claimant's account and confiscated his documents without discovering an objectionable image. If these facts are presumed to be true, Microsoft cannot benefit from Section 230 immunity, since there is no objectionable content that places Microsoft under the guise of the CDA.

Microsoft's failure to produce the image and failure to name one person who reviewed the flagged image is particularly egregious in light of the company's admission that the PhotoDNA program is prone to error. Microsoft alleges that PhotoDNA has an error rate of 1 in 50 billion scans, based on Dr. Hany Farid's single Congressional testimony. *See* MJOP, at 7; *see also* Exhibit D to Declaration of Natalie Nahabet in Support of Microsoft's Opposition to Claimant's Motion to Compel ("Nahabet Decl."). First, Claimant disputes that figure and seeks to engage in discovery to uncover the actual error rate for false positives. Second, Farid's statement in his Congressional testimony is not specific to *false positives*—which is the key metric relevant to Microsoft's bad faith behavior in this matter—but rather refers to errors. *See* Nahabet Decl., Exhibit D. In other words, Farid's statement regarding error rates does not adequately capture the number of false hits where PhotoDNA erred in falsely identifying an unobjectionable image as an objectionable one. Third, in his testimony, Farid does not offer the scientific or mathematical basis of his estimate of the error rate. This omission may only be cured with further discovery. *See id.* Fourth, Farid, a professor at Dartmouth, was one of the key developers of PhotoDNA—a professor who has staked a significant amount of his professional career and credibility on the efficacy of the PhotoDNA, and someone who benefits financially from the success of PhotoDNA, maintains deep bias and is laden with conflicts of interest. Fifth, even if Farid's analytics were correct when he performed them, it does not follow that the data remains true today since the volume of images has increased significantly and the ability to manipulate images has complicated and compromised the accuracy of scanning algorithms such as PhotoDNA. Sixth, by Microsoft's admission in this arbitration, images stored on OneDrive that were shared already and scanned (and hence cleared as non-CSEAI) were *rescanned* by PhotoDNA as the recap function falsely marked them as shared. *See* Supplement, ¶ 1-5. This rescanning of images which had already been cleared of CSEAI,

massively changes the denominator in the fraction of how many errors PhotoDNA makes. Microsoft has failed to disclose any indication so far as to the extent of that rescanning, and hence the critical need to understand that true denominator of the error rate.

Indeed, even assuming *arguendo* Microsoft's 1 in 50 billion error rate, the frequency of false hits is alarming. Over 3 billion images are shared on the internet each day.¹ With PhotoDNA, that would translate to a false positive hit approximately twice a month. At one point in this arbitration Microsoft indicated that PhotoDNA scans 1.8 billion images each day. *See* Davis Aff. at 3. Thus, even if all the rosiest projections of PhotoDNA were stipulated to at a 1 in 50 billion error rate (which Claimant strenuously objects to as a fact), PhotoDNA would falsely identify an image shared via OneDrive every 27.77 days, or approximately at least 13 false positives per year. Alternatively, if PhotoDNA's error rate were 1 in 1.8 billion, PhotoDNA would falsely flag a CSEAI every day of the year.

A motion for judgment on the pleadings can be granted “only if no relief could be granted under any set of facts that could be proved.” *Syncsort*, 50 F. Supp. 2d at 324. A claim should not be dismissed unless it appears beyond doubt that “the facts alleged in the complaint, even if true, fail to support the claim.” *Id.* at 325 (citations omitted). As New Jersey courts explain, in reviewing the sufficiency of a claim on a motion for judgment on the pleadings, a court or arbitrator has a limited role: “The issue is not whether a plaintiff will ultimately prevail but whether the claimant is entitled to offer evidence to support his [or her] claims.” *Id.*

¹ See T.J. Thomson, et al., *3.2 Billion Images and 720,000 Hours of Video are Shared Online Daily*, THE CONVERSATION (Nov. 2, 2020). Available at: <https://theconversation.com/3-2-billion-images-and-720-000-hours-of-video-are-shared-online-daily-can-you-sort-real-from-fake-148630>.

Here, Claimant can succeed if, as he claims, there is no CSEAI and no objectionable image. Since facts must be presumed in Claimant's favor—and at the very least there is a material dispute of fact as to whether any image-at-issue is CSEAI—the motion should be denied.

B. There is a Material Dispute of Fact as to Whether Microsoft Conducted Human Review of the Flagged Image

Microsoft asserts that, in all instances where its computer program flags an image as CSEAI, the company conducts a human review of the image. *See* Microsoft's Opposition to Claimant's Motion to Compel, at 3, 5, 7-9; MJOP, at 3, 8, 11, 14. In Claimant's instance, however, Microsoft has indicated that it cannot name one person who actually reviewed any image-at-issue. *See* Exhibit A, Microsoft's Objections and Responses to Claimant's First Set of Interrogatories, at 2-3. As such, it is unclear if any person actually has reviewed the image, and unclear if any objectionable image actually exists. Discovery is necessary to uncover precisely who, if anyone, reviewed the image in this case, and what the reviewer(s) actually determined.

On a motion for judgment on the pleadings, the Arbitrator must “view the facts presented in the pleadings and the inferences to be drawn therefrom in the light most favorable to the nonmoving party.” *Wolfington*, 935 F.3d at 195. A motion for judgment on the pleadings can be granted “only if no relief could be granted under any set of facts that could be proved.” *Syncsort*, 50 F. Supp. 2d at 324. A claim should not be dismissed unless it appears beyond doubt that “the facts alleged in the complaint, even if true, fail to support the claim.” *Id.* at 325 (citations omitted). As New Jersey courts explain, in reviewing the sufficiency of a claim on a motion for judgment on the pleadings, a court or arbitrator has a limited role: “The issue is not whether a plaintiff will ultimately prevail but whether the claimant is entitled to offer evidence to support his [or her] claims.” *Id.*

By its own admissions, Microsoft cannot name one person who has reviewed the alleged CSEAI. *See* Exhibit A, Microsoft’s Objections and Responses to Claimant’s First Set of Interrogatories, at 2-3. Moreover, Claimant alleges that there is no CSEAI. *See* Fourth Amended Claim, at 5, 16-17. Claimant can succeed in this matter if, as he claims, there is no CSEAI, no objectionable image, and Microsoft failed to conduct a reasonable human review of the flagged image. Since facts must be presumed in Claimant’s favor—and at the very least there is a material dispute of fact as to whether any image-at-issue is CSEAI—the motion should be denied.

C. There is a Material Dispute of Fact as to Whether Microsoft Maintained Subjective Good Faith

Claimant alleges that Microsoft acted in bad faith in improperly and illegally scanning his private files, wrongfully closing his OneDrive account, wrongfully precluding him from accessing his files stored on OneDrive, and wrongfully confiscating thousands of his documents that are stored on OneDrive. *See* Fourth Amended Claim at 16-21. Indeed, many of Claimant’s allegations are already supported by Microsoft’s own admissions in this matter. *See, e.g.,* Supplement, ¶ 1-5.

As one example of bad faith, for nearly twelve months Microsoft alleged that Claimant shared CSEAI via OneDrive. However, after discovery commenced in this matter, Microsoft admitted that it was incorrect, and that Claimant did not share CSEAI via OneDrive or any other means. *See* Supplement, ¶ 1-5. In addition, for nearly twelve months Microsoft asserted that the company “does not search its customers’ private files. *See* Davis Aff., ¶ 9. As Davis further affirmed, “customer accounts remain private; it is only when data is shared by a customer that PhotoDNA becomes operative.” *Id.* Once discovery commenced, Microsoft admitted that this affirmation was false, and that the company scanned Claimant’s private files. *See* Supplement, ¶ 1-5. Both of these lies evince clear bad faith on the part of Microsoft and demonstrate that

Microsoft did not act in subjective good faith when it scanned Claimant's private files, closed his OneDrive account, and confiscated tens of thousands of his private documents. *See* Fourth Amended Claim, at 16-21. Specifically, for nearly one year Microsoft failed to conduct even a cursory review of Claimant's declarations that he had not even shared ANY images with third parties via OneDrive. *See id.* at 16-17. Claimant had to pursue these proceedings to prove to Microsoft that they had serious internal errors. Had Microsoft not engaged in such bad faith conduct, the factual predicates of this matter may have come to light months ago, thus minimizing the harms to Claimant (which are ongoing as of the date of this motion).

As a second example of bad faith, given the large number of false hits and the known fact that individuals will be falsely identified as having shared child pornography, it is absolutely essential that Microsoft conduct reasonable human review of all flagged images. But in the very limited and inadequate discovery provided by Microsoft, Microsoft has admitted that the company is unaware of ANY instance where a "human rejected PhotoDNA's determination" that an image was a match to an image in the CSEAI database. *See* Exhibit A, Microsoft's Responses to Claimant's First Set of Interrogatories, at 6. Microsoft's admission on this point is baffling. On the one hand, Microsoft admits that PhotoDNA makes mistakes and wrongly flags unobjectionable content as objectionable. On the other hand, Microsoft admits that the company has never overruled a decision of its computer program, PhotoDNA. *See id.* Moreover, through the very limited discovery conducted in this matter, Microsoft has admitted the company is willfully blind to collecting information on false positives. *See* Fourth Amended Claim at 19-21. Specifically, Microsoft indicated that the company "has not maintained records showing a "rate of PhotoDNA false-positives." *See* Exhibit A, Microsoft's Responses to Claimant's First Set of Interrogatories, at 4. This willful ignorance, along with knowingly falsely accusing its own customers of felonious

behavior is precisely why Microsoft's policies and procedures are tantamount to bad faith. And without further and appropriate discovery, only this tip of the iceberg will be seen by one Claimant, while countless other OneDrive users will have suffered false accusations and lost access to all of their irreplaceable personal files. Microsoft sums the effect of Microsoft's errors succinctly with their Interrogatory Response No. 2 that Microsoft "has not reactivated a OneDrive account that it permanently suspended and closed..." *See id.* at 4.

As a third example of bad faith, Microsoft specifically admits: "Based on the preserved metadata for the image that PhotoDNA flagged from Claimant's OneDrive account, Microsoft was able to confirm that this "recap" feature had changed the status of this image to "shared," causing PhotoDNA to scan the image." *See* Microsoft's Supplement, ¶ 1-5. Thus, after one year of alleging that Claimant shared CSEAI, based on discovery produced by Claimant, Microsoft could no longer hide behind its misrepresentation and willful blindness, and was forced to admit that Claimant did not communicate or share any objectionable image via OneDrive or any other means. Not only did Microsoft's own technology fail to conform to its own specifically devised policies and procedures, but compounding the bad faith is that Microsoft did not even review its own PhotoDNA scanning, even in the face of Claimant's near year-long denial that he shared any CSEAI via ANY communication method. Microsoft only reviewed its own automated, bad faith conduct after Claimant had proven, via incontrovertible evidence that he did not communicate ANY objectionable images or files via OneDrive. *See* Exhibit 1 to Claimant's Third Amended Claim. Without proper discovery to determine the universe of images that PhotoDNA was scanning, granting a judgment on the pleadings would allow Microsoft to admit guilt, but escape discovery or culpability for their actions that are not related to removing objectionable content.

As a fourth example of bad faith, Microsoft has falsely accused Claimant of maintaining and distributing child pornography by neglecting to conduct a good faith review of his initial position that he did not possess or share CSEA. *See* Fourth Amended Claim, at 16-17. These false accusations unquestionably and predictably have caused significant personal and professional harm to Claimant. *See id.* at 21.

A fifth example of Microsoft's bad faith is the company's failure to follow the protocols outlined in the MSA regarding disputes with OneDrive customers. *See* Fourth Amended Claim, at 7. Specifically, the MSA states that Microsoft will engage in good faith efforts to resolve customer disputes. *See id.* Here, rather than engage in even cursory good faith efforts to attempt to resolve Claimant's query regarding why Microsoft abruptly closed his account, the company simply ignored Claimant's inquiries and all standards of due process, entirely placing the burden on Claimant to seek relief through this forum. *See id.* Microsoft failed to provide any explanation for its egregious conduct for four months until they were compelled to by these proceedings.

Although Microsoft goes to great lengths to portray its actions in this matter to qualify as subjective good faith, those conclusory and self-serving statements are belied by the factual record and the allegations in the Fourth Amended Claim. Moreover, Microsoft's false affirmations and admitted breaches of its own policies objectively constitute bad faith. At the very least, based on Claimant's allegations and the limited discovery produced to date, a material dispute of fact exists as to whether Microsoft acted in bad faith.

As courts have recognized, under Section 230 of the CDA, it is clear from "statutory language, history, and case law [] that providers do not have unfettered discretion to declare online content 'objectionable.'" *Enigma Software Grp. USA, LLC v. Malwarebytes, Inc.*, 946 F.3d 1040, 1047 (9th Cir. 2019), *cert. denied*, 141 S. Ct. 13 (2020). And courts should not permit "an

‘unbounded’ reading of the phrase ‘otherwise objectionable.’” *Id.* at 1049 (citing *Zango, Inc. v. Kaspersky Lab, Inc.*, 568 F.3d 1169, 1178-80 (9th Cir. 2009)). Moreover, “the fact that the statute requires the user or service provider to subjectively believe the blocked or screened material is objectionable does not mean anything or everything [a defendant] finds subjectively objectionable is within the scope” of Section 230 of the CDA. *Song fi Inc. v. Google, Inc.*, 108 F. Supp. 3d 876, 884 (N.D. Cal. 2015).

On a motion for judgment on the pleadings, the Arbitrator must “view the facts presented in the pleadings and the inferences to be drawn therefrom in the light most favorable to the nonmoving party.” *Wolfington*, 935 F.3d at 195. A motion for judgment on the pleadings can be granted “only if no relief could be granted under any set of facts that could be proved.” *Syncsort*, 50 F. Supp. 2d at 324. A claim should not be dismissed unless it appears beyond doubt that “the facts alleged in the complaint, even if true, fail to support the claim.” *Id.* at 325 (citations omitted). As New Jersey courts explain, in reviewing the sufficiency of a claim on a motion for judgment on the pleadings, a court or arbitrator has a limited role: “The issue is not whether a plaintiff will ultimately prevail but whether the claimant is entitled to offer evidence to support his [or her] claims.” *Id.*

Based on these well-established principles—and because there is a material dispute of fact as to whether Microsoft maintained subjective good faith in scanning Claimant’s private files, closing his account, and confiscating tens of thousands of his documents—the motion should be denied.

V. The MJOP Does Not Seek to Dismiss All Claims in this Arbitration

It is essential to highlight that Microsoft’s motion for judgment on the pleadings does not seek to dismiss all claims in this arbitration. In its own motion papers, Microsoft does not present

any argument that Section 230 immunity serves to dismiss the allegations in the Third Amended Claim (which are not altered by the Fourth Amended Claim) regarding the negligence and breach of contract claims surrounding Microsoft's faulty Windows software update that necessitated the reinstallation of Windows and wiped Claimant's hard drive. *See* MJOP. Rather, Microsoft dedicates the motion entirely to Claimant's claims regarding his OneDrive account. Claimant's negligence and breach of contract claims surrounding Microsoft's faulty software update were present in the Third Amended Claim, *see* Claimant's Third Amended Claim at 8-9, and not altered by the Fourth Amended Claim. *See* Fourth Amended Claim at 8-9.

Accordingly, in its Reply for the motion for judgment on the pleadings, Microsoft is precluded from raising or arguing any new issue not previously raised that could have been raised in its initial motion papers. As the Third Circuit has unambiguously held: "A moving party may not raise new issues and present new factual materials in a reply brief that it should have raised in its initial brief. *See International Raw Materials, Ltd. v. Stauffer Chem. Co.*, 978 F.2d 1318, 1327 n. 11 (3d Cir.1992) (refusing to consider an issue raised for the first time in a reply brief).

Because Microsoft elected not to include, in its MJOP, the claims regarding Microsoft's faulty software update, those claims must necessarily survive this MJOP.

VI. Insofar as the Motion Is Granted Due to a Pleading Deficiency, Claimant Respectfully Requests Leave to Amend the Pleadings

Insofar as the motion is granted due to a pleading deficiency that may be cured, Claimant respectfully requests leave to amend the pleadings. As courts in New Jersey have consistently and routinely held, "leave to amend a pleading shall be freely given in the interest of justice." *Hansen v. Hansen*, 770 A.2d 1278, 1286 (N.J. App. Div. 2001) (internal quotes omitted). Moreover, "motions for leave to amend should be treated indulgently and leave should be freely given in the

interest of justice.” *Id.* (citing *Kernan v. One Washington Park*, 154 N.J. 437, 456–57 (N.J. 1998)). Here, justice requires that Microsoft be held accountable for its improper and bad faith conduct, where the company wrongfully scanned Claimant’s private files, wrongfully closed Claimant’s OneDrive account, wrongfully precluded Claimant from accessing his private files stored on OneDrive, and wrongfully confiscated thousands of Claimant’s private documents that are stored on OneDrive. Given this egregious conduct, to the extent the motion is granted due to a pleading deficiency that may be cured, Claimant respectfully requests that the Arbitrator grant leave to amend the claim.

CONCLUSION

For the reasons outlined herein, Claimant respectfully requests that the Arbitrator deny Microsoft’s motion for judgment on the pleadings.

Dated: June 8, 2021

SALZANO, LAMPERT & WILSON, LLP

By: /s/ Frank Salzano

Frank Salzano, Esq. (NY SBN 4114849)
275 Madison Avenue, 35th Floor
New York, New York 10016
(646) 863-1883
fsalzano@slwlawoffices.com

Attorneys for Claimant

EXHIBIT 24

AMERICAN ARBITRATION ASSOCIATION

THOMAS DEUTSCH, ESQ.,	:	
	:	
<i>Claimant,</i>	:	CASE NO. 01-20-0014-3715
	:	
v.	:	
	:	
MICROSOFT CORPORATION,	:	
	:	
<i>Respondent.</i>	:	

RESPONDENT MICROSOFT CORPORATION’S REPLY IN SUPPORT
OF MOTION FOR JUDGMENT ON THE PLEADINGS
ON FOURTH AMENDED DEMAND

Table of Contents

I. INTRODUCTION	3
II. ANALYSIS	4
a. Section 230(c)(2)(A) Grants Microsoft Immunity for Blocking “Access to or Availability of Material” in OneDrive.	4
i. The Plain Language and Legislative History of Section 230 Confirm that Section 230(c)(2)(A) Applies Regardless Whether the Blocked Content Was Published or Shared.	4
ii. Case Law also Confirms that Section 230(c)(2)(A) Applies Regardless Whether the Blocked Content Was Published or Shared.	7
b. Microsoft’s OneDrive is an Interactive Computer Service.	9
c. Claimant’s Own Allegations Demonstrate that Microsoft Acted in Good Faith When It Blocked Claimant’s Account.	11
d. The Arbitrator Should Dismiss the Fourth Amended Demand Without Leave to Amend a Fifth Time.	14
III. CONCLUSION	15

I. INTRODUCTION

Microsoft blocked Claimant’s OneDrive because it detected in the account, through its standard processes, an image that Microsoft “considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable,” 47 U.S.C. § 230(c)(2)(A)—namely an image that Microsoft believed to be child sexual exploitation and abuse imagery. Because Microsoft prohibits consumers from using its services to “engage in any activity that exploits, harms, or threatens to harm children,” it permanently suspended Claimant’s account under the MSA. MSA Code of Conduct ¶ 3.a.ii; *see also id.* at ¶ 3.a.ix. That is precisely the good faith “private blocking and screening of offensive material” that Congress intended Section 230 to protect. 47 U.S.C. § 230 (title). Claimant does not dispute that Section 230(c)(2)(A) allows providers to block in good faith material they subjectively believe to be objectionable.

Instead, he primarily (a) argues he did not “share” the child sexual exploitation and abuse material through OneDrive, so Section 230(c)(2)(A) does not apply; (b) claims OneDrive is not an “interactive service”; and (c) complains that Microsoft scanned his privately stored content. But if Claimant were right that Section 230(c)(2)(A) does not apply in these circumstances—i.e., to a blocking action taken by a cloud-storage service that “provides or enables computer access by multiple users to a computer server”—that would upend the very purposes of the statute. *Id.* at § 230(f)(2). Indeed, the stated intent of Section 230 is “to remove disincentives for the development and utilization of blocking and filtering technologies” and “to ensure vigorous enforcement of Federal criminal laws to deter and punish trafficking in obscenity.” *Id.* at § 230(b)(4)-(5). The rule Claimant advocates would disincentivize service providers such as Microsoft from developing and using blocking and filtering technologies and that, in turn, would reduce law enforcement’s ability to deter and punish perpetrators. This, in turn, would mean individuals could possess child sexual exploitation and abuse materials online without risk of detection by service providers so long as they store that content in private computer files.

Patently, that is not the intended outcome of Section 230. And this is apparent from the face of the statute. Section 230(c)(2)(A) expressly immunizes “any action voluntarily taken in good faith to *restrict access to or availability of material*” the provider “considers” to be “objectionable”—such as child sexual exploitation and abuse material. *Id.* at § 230(c)(2)(A) (emphasis added). By blocking Claimant’s account, Microsoft restricted “access to or availability of” material that it “considers to be ... objectionable” and that it prohibits under the MSA’s Code of Conduct. Further, Microsoft did so through standardized processes and procedures, including through the (highly accurate) PhotoDNA technology and Microsoft’s standard human

confirmation process, both of which apply in a uniform fashion, without regard to the particular individual account. Tellingly, although Claimant has received discovery from Microsoft in this matter, he still does not allege any facts showing Microsoft targeted him specifically. Nor could he, as the express terms of the MSA, including the MSA's Privacy Statement, permitted Microsoft to apply these standard processes and procedures to content in Claimant's OneDrive, whether stored in "private" or "shared" folders. MSA Privacy Statement at p. 8.

Microsoft acted in good faith when, consistent with the MSA's Code of Conduct and Privacy Statement, it blocked Claimant's OneDrive upon detecting in the account content that Microsoft believes is "obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable" and that is prohibited by the MSA's Code of Conduct. 47 U.S.C. § 230(c)(2)(A); MSA Code of Conduct ¶ 3.a.ii & ix. For the reasons set forth in its Motion for Judgment on the Pleadings and here, the Arbitrator should grant judgment on the pleadings as to all claims, including those alleged in the Fourth Amended Demand, to which Section 230(c)(2)(A) applies for all the same reasons it applies to the Third Amended Demand.

II. ANALYSIS

a. Section 230(c)(2)(A) Grants Microsoft Immunity for Blocking "Access to or Availability of Material" in OneDrive.

Claimant does not dispute that Section 230(c)(2)(A) affords interactive computer service providers broad immunity when they "restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable." 47 U.S.C. § 230(c)(2)(A). Nor does he point to *any* language in Section 230 showing this grant of immunity applies only to actions taken to block content that was published, shared, or communicated over the internet, and not to content that was stored on the internet (and therefore susceptible to sharing through other means). Instead, he boldly asserts that "Section 230 immunity only applies to actions taken by an interactive service provider where the provider seeks to remove information that was *shared* with third parties." Opp. at 11 (emphasis in original). The plain language of the statute, the policies underlying it, and the case law all confirm otherwise.

i. The Plain Language and Legislative History of Section 230 Confirm that Section 230(c)(2)(A) Applies Regardless Whether the Blocked Content Was Published or Shared.

When interpreting a statute, we "need to 'discern legislative intent,' considering first the plain meaning of the statutory text." *Lawrence v. City of Philadelphia, Pa.*, 527 F.3d 299, 316-17

(3d Cir. 2008) (citation omitted). “The plain meaning of the text should be conclusive, except in the *rare* instance when the court determines that the plain meaning is ambiguous.” *Id.* (emphasis added). The plain language of Section 230 is clear and unambiguous. The statute, by its very title, provides “[p]rotection for private blocking and screening of offensive material.” 47 U.S.C. § 230 (title). Section 230(c) contains the immunity provisions and, again, specifies the statute’s purpose: “Protection for ‘Good Samaritan’ blocking and screening of offensive material.” *Id.* at § 230(c). Section 230(c) grants immunity for two types of blocking and screening:

(1) Treatment of publisher or speaker

No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.

(2) Civil Liability

No provider ... of an interactive computer service shall be held liable on account of—

(A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider ... considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or

(B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1)....

Id. While Section 230(c)(1) applies to a provider’s editorial decisions regarding published or communicated content, Section 230(c)(2)(A)—the only ground on which Microsoft moves here—is not so limited.

Quite the contrary, nothing in Section 230(c)(2)(A) excludes from immunity a provider’s action to “restrict access to or availability of material that the provider ... considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable” and that is stored in a “private” folder in an online service. Rather, Section 230(c)(2)(A) broadly covers “any action” a provider engages in “to restrict access to or availability of material.” *Id.* This necessarily includes Claimant’s own “access to” material that Microsoft “considers ... to be objectionable” and expressly prohibits on its services. *Id.* If Congress had intended Section 230(c)(2)(A) to grant immunity only for actions taken to “restrict access to or availability” of public, “shared,” or communicated information, it would have done so, as it has in numerous other instances. *See, e.g.*, 18 U.S.C. § 876 (criminalizing any deposit “to be sent or delivered” via US

mail demanding ransom); 52 U.S.C. § 30104(f) (reporting requirement for “electioneering communications”).

Indeed, this is precisely what Congress did in Section 230(c)(1), which applies when a litigant seeks to hold a service provider liable as a “publisher” or “speaker” of a third party’s content, i.e., to published or communicated information.¹ Congress knew how to limit Section 230(c)(2)(A) to published or communicated information—yet it did not. *See Levitt v. Yelp! Inc.*, 2011 U.S. Dist. LEXIS 124082, at *23-24 (N.D. Cal. Oct. 26, 2011) (“Where Congress includes particular language in one section of a statute but omits it in another ..., it is generally presumed that Congress acts intentionally and purposely in the disparate inclusion or exclusion.”) (citing *Keene Corp v. U.S.*, 508 U.S. 200, 208 (1993)) (internal quotations omitted). Instead, Section 230(c)(2)(A) grants immunity to “any action” taken to “restrict access to or availability of material,” without requiring that the material first have been published, shared, communicated, or otherwise made public.

Surrounding statutory text and legislative history support this plain language interpretation of Section 230(c)(2)(A). In interpreting a statutory provision, the court should “look to the provisions of the whole law, and to its object and policy.” *John Hancock Mut. Life Ins. Co. v. Harris Tr. & Sav. Bank*, 510 U.S. 86, 94–95 (1993). Congress enacted Section 230 to codify “the policy of the United States” of “promot[ing] the continued development of the Internet and other interactive computer services” and “preserv[ing] the vibrant and competitive free market that presently exists for the Internet.” 47 U.S.C. § 230(b). To effectuate those goals, Congress designed Section 230 broadly “to remove disincentives for the development and utilization of *blocking and filtering technologies*” and “to ensure vigorous enforcement of Federal criminal laws to deter and punish in trafficking in obscenity ... by means of computer.” *Id.* at § 230(b)(4), (5) (emphasis added). As Microsoft explained in its Motion, the statute accomplishes these goals through a quid pro quo: “in return for [Congress conferring upon computer service providers] th[e] protection ... that they wouldn’t be sued indiscriminately,” the providers were to be “responsible in terms of policing their platforms.” Mot. at 5 (quoting Alina Selyukh, *Section 230: A Key Legal Shield for Facebook, Google Is About to Change*, NPR (Mar. 21, 2018) (quoting Senator Wyden)). Respecting the balance Congress struck, “courts have construed the immunity provisions in § 230 broadly” and interpret “close cases ... in favor of immunity.” *Jones v. Dirty World Entm’t Recordings LLC*, 755 F.3d 398, 408 (6th Cir. 2014).

¹ “[T]he very essence of publishing is making the decision whether to print or retract a given piece of content.” *Bennet v. Google, LLC*, 882 F.3d 1163, 1167 (D.C. Cir. 2018).

Claimant identifies nothing in the statute’s plain language or legislative history evincing an intent to carve out from these policy goals objectionable material such as child sexual exploitation and abuse imagery that an individual stores online, but may not have published, shared, or communicated online yet. Indeed, a contrary rule would mean service providers would have to *wait* until an individual *distributes* child sexual exploitation and abuse material before the provider could be protected from suit. Fortunately, the statute immunizes actions taken to “restrict access to or availability of the material” without regard to the point in time the blocking action was taken, ensuring immunity for blocking “access to” material so that it may not also be published or shared.

Claimant rests his arguments otherwise on a self-selective recasting of the history of Section 230, based entirely on the Congressional response to *Stratton Oakmont, Inc. v. Prodigy Services Co.*, No. 31063/94, 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995). *Stratton* held that once a service provider undertook to filter offensive content from its network, the provider assumed responsibility for any offensive content it failed to filter, even if it lacked knowledge of the content. Opp. at 10. According to Claimant, Congress adopted Section 230 exclusively “to perform some editing on user-generated content without thereby becoming liable.” *Id.* From there, he argues “Section 230 immunity applies *solely* to instances where ‘the cause of action necessarily requires that the defendant be treated as the publisher or speaker of content provided by another.’” *Id.* at 13.

But that is the purpose of Section 230(c)(1)—*not* Section 230(c)(2)(A). *Zango, Inc. v. Kaspersky Lab, Inc.*, 568 F.3d 1169, 1173-74 (9th Cir. 2009) (“Section 230(c)(1) directly aimed at the problem created by the *Stratton* decision”). Microsoft does not invoke Section 230(c)(1) here. Rather, it seeks dismissal under Section 230(c)(2)(A). Microsoft has shown here and in its Motion that Section 230(c)(2)(A) fulfills distinct statutory purposes from Section 230(c)(1). *See* Mot. at II.a. Claimant offers no response. Instead, he ignores the text and legislative history of Section 230(c)(2)(A). That, of course, runs counter to basic principles of statutory interpretation.

ii. Case Law also Confirms that Section 230(c)(2)(A) Applies Regardless Whether the Blocked Content Was Published or Shared.

Section 230 case law further supports Microsoft’s plain language interpretation of Section 230(c)(2)(A). In *Domen v. Vimeo*, for instance, the Second Circuit upheld the district court’s Rule 12(b)(6) dismissal under Section 230(c)(2)(A) not because the user had shared the content with others on Vimeo, but because Vimeo subjectively believed the content was objectionable and in violation of its terms of use. *See* 991 F.3d 66, 72 (2d Cir. 2021). So too in *Holomaxx Techs. v. Microsoft Corp.* 783 F. Supp. 2d 1097, 1104 (N.D. Cal. 2011). There, the court made clear that “a

provider's subjective determination of what is 'objectionable'" controls the Section 230(c)(2)(A) analysis. *Id.* The court held Section 230(c)(2)(A) immunity applied and dismissed the claims because it was "clear from the allegations of the complaint itself that Microsoft reasonably could conclude that Holomaxx's e-mails were 'harassing' and thus 'otherwise objectionable.'" *Id.* In neither case did the court rest its analysis under Section 230(c)(2)(A) on whether the user had "shared" or "published" the content. Rather, the courts rightly focused on the plain words of the statute, analyzing whether the providers blocked the accounts upon identifying content the providers "consider[ed]" to be objectionable, and whether the providers took these blocking actions consistent with their terms of use. Claimant's attempt to limit Section 230(c)(2)(A) to blocking only "shared" content finds no support in the case law.

The mere fact that these and other cases did involve "publicly available" or published content does not narrow the plain language or legislative intent of Section 230(c)(2)(A), as Claimant attempts to suggest. *See* Opp. at 14. Rather, this simply reflects that the more commonly litigated fact pattern under Section 230 is that involving published or posted content online. And in any event, courts *have* applied Section 230(c)(2)(A) even where the blocked content had not been published, communicated, or shared online. In *Zango*, for example, a distributor of Internet security software was sued by an online media company for restricting customer access to downloadable programs. 568 F.3d at 1170. There was thus no "*publisher* or *speaker* of content shared by any third party." Opp. at 17 (emphasis added). Still, the Ninth Circuit held "the statute plainly immunizes from suit a provider of interactive computer services that makes available software that filters or screens material that the user or the provider deems objectionable." *Id.* at 1173. Likewise, in *Smith v. Trusted Universal Standards in Elec. Transactions*, Microsoft's spam and virus filtering software blocked email communications before they were ever sent (i.e., before they were "shared"). 2011 WL 900096, at *1 (D.N.J. Mar. 15, 2011). There too, Microsoft was entitled to immunity under Section 230 for preventing a user from sharing objectionable content.

Similar to the blocking actions in *Zango* and *Smith*, Microsoft here blocked "access to or availability of" material it "considers to be ... objectionable" (including restricting "access" by Claimant himself), which is all the statute requires (and which prevented the child sexual exploitation and abuse material from being published, communicated, or shared on or from Microsoft's services).²

² Each of the four cases Claimant cites for the proposition that Section 230 has a "limited reach" involved claims of immunity under Section 230(c)(1). *See* Opp. at 17. Again, Microsoft does not move under

b. Microsoft’s OneDrive is an Interactive Computer Service.

OneDrive is an interactive computer service under Section 230 because it gives users access to a computer server and allows users to upload, view, and share images and files. *See* Mot. at IV.a. Claimant seeks to circumvent this by suggesting this inquiry turns on how *he* used OneDrive in *this* instance. *See, e.g.*, Opp. at 16 (arguing OneDrive does not qualify as an “interactive service” for “consumer accounts whose contents are not shared at all”). Not so.

Section 230 defines “interactive computer service” as “any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet....”³ 47 U.S.C. § 230(f)(2). OneDrive indisputably provides users with online access to a cloud server on which users can store (as well as share or publish) content. *See* <https://www.microsoft.com/en-us/microsoft-365/onedrive/free-online-cloud-storage/> (“Store your files and photos with OneDrive...cloud storage and access them from any device, anywhere.”; “Share your files and photos with friends and family.”). OneDrive thus “provides or enables computer access by multiple users to a computer server.” 47 U.S.C. § 230(f)(2). That suffices regardless whether Claimant shared the specific image that gave rise to the account block in this case—the statute does not limit the definition of “interactive service provider” to services actually used to share or publish content in the particular case before the court. And even if the statute did so limit “interactive service provider,” Claimant’s own pleadings in this case confirm he *did* in fact use OneDrive to store and share content. *See* Third Amended Demand, Ex. 2 (screenshot Claimant filed showing he “shared” content in his OneDrive). Claimant cites no authority for the notion that a computer service falls in and out of the definition of an “interactive service provider” based on how the user chose to use the service in the particular use-case before the court—nor would such a rule be workable. On the contrary, all that is required is “computer access by multiple users to a computer server.” 47 U.S.C. § 230(f)(2).

Indeed, “reviewing courts have treated § 230(c) immunity as quite robust, adopting a relatively expansive definition of ‘interactive computer service....’” *Carafano v. Metrosplash.com, Inc.*, 339 F.3d 1119, 1123 (9th Cir. 2003)). So, in *Smith*, the court explained

Section 230(c)(1), so none of these apply. Nor do any of these cases hold that Section 230(c)(2)(A) applies only when the restricted content had first been published, communicated, or shared by the blocked user before the block. *See, e.g., id.* (citing *Enhanced Athlete Inc. v. Google LLC*, 2020 WL 4732209 at *1 (N.D. Cal. Aug. 14, 2020) (acknowledging Section 230(c)(1) and (c)(2) fulfill different purposes)).

³ Claimant implies that Microsoft’s citation to the categories of providers identified in *LeadClick* was somehow an admission that these categories are exclusive. *See* Opp. at 17. Microsoft made no such admission or representation; nor are the plain words of the statute so limited. *See* 47 U.S.C. § 230(f).

that “websites are considered interactive computer services because they allow numerous users to *access and use* their services....,” regardless whether users also publish or share content on those websites. 2011 WL 900096, at *5 (emphasis added) (citing *Fair Housing Council of San Fernando Valley v. Roommates.Com, LLC*, 521 F.3d 1157, 1162 n. 6 (9th Cir. 2008) (defendant’s website was an “interactive computer service” because although it did not provide or enable access to the Internet, “[t]hrough the Internet, many thousands of members are able to access and use a searchable database maintained on [the defendant’s] computer services”)). The same holds true here: Claimant nowhere disputes that OneDrive allows “numerous users to access and use” its services, including to store and share content, and nor could he, having admittedly used OneDrive in these very ways.

In addition, Section 230 defines an “interactive computer service” as including an “access software provider.” 47 U.S.C. § 230(f)(2). Under Section 230, an “access software provider” is “a provider of software (including client or server software), or enabling tools that do any one or more of the following: ... (A) filter, screen, allow, or disallow content; ... or (C) transmit, receive, display, forward, cache, search, subset, organize, reorganize, or translate content.” *Id.* at § 230(f)(4). OneDrive provides server software that allows the transmission, receipt, display, forwarding, caching, searching, organizing and reorganizing of content. *See, e.g.*, <https://www.microsoft.com/en-us/microsoft-365/onedrive/online-cloud-storage> (“access, edit, and share your files”; “[s]tay connected, share your documents and photos with friends and family”; “[s]tore important files and photos”). Indeed, Claimant admits he used OneDrive to transmit his files to the cloud and to “reorganize[e] [his] files on OneDrive as well as continuing to add and modify documents, [and] data ...”. Fourth Amended Claim at 1. For this reason, too, OneDrive qualifies as an “interactive computer service” under Section 230.

It makes no difference that Claimant chose to pay a fee to obtain more storage in OneDrive. *See* Opp. at 13; *id.* at 12, 14 (arguing Section 230 does not apply to paid cloud storage services). Neither the statute nor the case law excludes paid online services from Section 230 immunity. Quite the contrary, in *Vimeo*, the Second Circuit upheld a motion to dismiss under Rule 12(b)(6) on Section 230 grounds despite the fact the plaintiff there had upgraded to a professional account, “which require[d] a monthly fee in exchange for access to more features and bandwidth.” 991 F.3d at 69. This makes good sense, as Claimant’s contrary rule would incentivize service providers to take blocking actions only on free services, which, in turn, would incentivize perpetrators to simply upgrade to paid services to avoid detection—an outcome that would

undermine Congress’s intent. The Arbitrator should reject Claimant’s invitation to gut Section 230 in this way.

c. Claimant’s Own Allegations Demonstrate that Microsoft Acted in Good Faith When It Blocked Claimant’s Account.

To overcome Section 230(c)(2)’s broad grant of immunity, plaintiff must plead “an absence of good faith.” Mot. at 11 (citing *Holomaxx*, 783 F. Supp. at 1105 (dismissing claims under Section 230(c)(2) because plaintiff failed to allege “facts in support of its conclusory claim that Microsoft’s filtering program is faulty, nor [did] it identify an objective industry standard that Microsoft fail[ed] to meet”)). As Microsoft showed in its Motion, *id.* at 11-15, Claimant has not met this pleading burden—and this holds true for both the Third and Fourth Amended Demand. Both Demands rely on the MSA. *See, e.g.*, Third Amended Demand at §§ II-V; Fourth Amended Demand at §§ II-V, VIII, X. The MSA’s Privacy Statement expressly allowed Microsoft to apply its standard scanning and human confirmation review processes to content in OneDrive, whether stored in “private” or “shared” folders, and the MSA’s Code of Conduct expressly allowed Microsoft to permanently suspend Claimant’s OneDrive when Microsoft detected and confirmed, through those standard processes, content in the account that violated the Code of Conduct (i.e., child sexual exploitation and abuse imagery). *See* Mot. at 7-8; MSA Code of Conduct ¶¶ 3.a.ii, ix, 3.b; MSA Privacy Statement at 8. Claimant’s own allegations and documents relied on in his Demands establish that Microsoft acted in good faith.

Even assuming having PhotoDNA scan Claimant’s private OneDrive folder was a mistake (and it was not given the MSA’s Privacy Statement and Code of Conduct do not limit Microsoft’s scanning activities to “shared” content), under well-established Section 230 case law, that still does not evidence a lack of good faith. *See* Mot. at 12-14 (citing and discussing *Vimeo*, 991 F.3d 66 and *e360Insight, LLC v. Comcast Corp.*, 546 F. Supp. 2d 605 (N.D. Ill. 2008)); Opp. at 26, 28 (arguing bad faith on this basis). And even if Microsoft mistakenly skipped the human review step in this case (and it did not, as Microsoft’s discovery response showed, Opp. at Ex. A at pp. 3, 6), again, that mistake would not constitute an absence of good faith under Section 230. *See* Mot. at 14 (citing *Vimeo*, 991 F.3d at 68 and *e360Insight*, 546 F. Supp. at 609); Opp. at 27, 29 (arguing bad faith on this basis). Claimant makes no other factual allegation of bad faith by Microsoft in blocking his account—despite having already received discovery from Microsoft. The Arbitrator should reject Claimant’s bad faith arguments.

As a threshold matter, and as Microsoft explained, *see* Mot. at 15, Microsoft’s alleged conduct *after* blocking Claimant’s account is irrelevant to the good faith analysis under Section

230. *See* 47 U.S.C. § 230(c)(2)(A) (referring to “any action voluntarily taken in good faith to restrict access to or availability of material,” not after the fact). This disposes of Claimant’s “bad faith” arguments based on Microsoft’s filings in this case (Opp. at 26-27), Microsoft’s factual investigation during this litigation (Opp. at 28-29), and Microsoft’s decision not to provide the basis for the account closure for four months after suspending his account (*id.*). And as Microsoft showed, under Section 230 it had no obligation to “discuss in detail its reasons for blocking [Claimant’s OneDrive] or to provide a remedy for such blocking,” as such a rule “would be inconsistent with the intent of Congress to ‘remove disincentives for the development and utilization of blocking and filtering technologies.’” Mot. at 15 (citing *Holomaxx*, 783 F. Supp. 2d at 1106).⁴

That leaves Claimant with two primary complaints: Microsoft scanned a private folder and the image might not be CSEAI. Opp. at 18, 22; Fourth Amended Demand at 16-18 (alleging claims based on Microsoft scanning a private folder). Neither suffices. Rather, under Section 230, to survive the pleading stage, Claimant must allege he was targeted or subjected to anticompetitive behavior, or that Microsoft failed to comply with industry standards. *See* Mot. at 14-15. Claimant alleges no such things; nor could he.

Microsoft complied with its Privacy Statement and Code of Conduct when it detected and confirmed through its standard processes CSEAI in Claimant’s private OneDrive folder and blocked his account as a result. The MSA’s Privacy Statement and Code of Conduct expressly informed Claimant that Microsoft (a) prohibits activity that “exploits harms, or threatens to harm children,” or “violates the privacy of others” on its services; and (b) “systematically scan[s] content in an automated manner” in OneDrive “to identify ... abusive actions.” Mot. at 6-7 (citing and discussing MSA Code of Conduct ¶ 3.a.ii & ix, and MSA Privacy Statement at 8); *see also id.* at 7 (citing MSA Privacy Statement at 9-10; MSA Code of Conduct ¶ 3.b; MSA ¶ 1).

Claimant does not dispute these facts. Nor does he identify, either in his Fourth Amended Demand or Opposition, a single provision in the MSA or its Privacy Statement prohibiting Microsoft from scanning private folders in OneDrive. He does not because no such provision exists. Instead, Claimant rests his theory on a Microsoft internal policy. But “internal policies do not establish the legal duty.” *Decker v. Target Corp.*, 2018 WL 4956641, at *2 (D. Utah Oct. 12, 2018) (citation and quotation omitted). In any event, at most the existence of this policy simply

⁴ Regardless, the record shows Microsoft promptly disclosed the feature that had triggered PhotoDNA scans of private folders in OneDrive, including in Claimant’s case, and attempted in good faith to resolve this matter by offering to remove and delete the offending image and restore access to Claimant’s OneDrive—relief Claimant rejected because he insists on forcing Microsoft to distribute CSEAI.

evidences that Microsoft mistakenly ran PhotoDNA on private folders in OneDrive—and it mistakenly did so for any user content identified by the recap feature, not just Claimant’s. Supp. Answer ¶¶ 2-4. “Under the law, a mistaken choice to block, if made in good faith, cannot be the basis for liability under federal or state law.” Mot. at 14 (*e360Insight*, 546 F. Supp. at 609).

Claimant’s insistence that this might be the 1 in 50 billion false-positive case likewise does not establish a lack of good faith. Claimant does not seriously dispute that he knows exactly what the offending image is or that it is the very same image a Dutch Court reviewed and concluded was illegal CSEAI. Instead, he complains that Microsoft has not identified who confirmed the image to be CSEAI or proven to his satisfaction that it was CSEAI. But what matters under Section 230(c)(2)(A) is not whether Microsoft accurately identified CSEAI, but rather whether it *subjectively* believed the content was objectionable and acted in good faith by using standardized protocols to identify and block it, consistent with the MSA. Mot. at 11-14. Section 230 “does not require that the material actually be objectionable; rather it affords protection for blocking material ‘that the provider or user *considers to be*’ objectionable.” *Zango*, 2007 WL 5189857, at *4 (W.D. Wash. Aug. 28, 2007) (emphasis added) *aff’d*, 568 F.3d 1169 (9th Cir. 2009). Claimant does not deny that this is the inquiry under Section 230.

To that end, Claimant readily acknowledges that his account was identified and suspended based on an “automated flagging system,” Opp. at 11, and nowhere disputes that PhotoDNA is industry standard, Mot. at 14-15. He also offers no *factual* allegation disputing that Microsoft followed its standard, anonymized human confirmation process here. See Opp. at Ex. A at pp. 3, 6.⁵ There is no authority for the notion that to obtain immunity under Section 230, a service provider must identify the specific individual who confirmed the content moderation decision.

At bottom, Microsoft followed the MSA’s Privacy Statement and Code of Conduct (both of which Claimant incorporates by reference in his Third and Fourth Amended Demands), and its standard processes and procedures when it (a) scanned content in Claimant’s OneDrive (i.e., user-generated content) against a database of hashes of known images of child sexual abuse that have been identified by NCMEC and Microsoft as the “worst of the worst” child pornography images;

⁵ Claimant seeks to muddy the waters by mischaracterizing Microsoft’s interrogatory responses. Opp. at 25, 27. As Microsoft explained in those responses, “no Microsoft employee accessed Claimant’s OneDrive account to review any particular image,” meaning no Microsoft employee logged into Claimant’s OneDrive to identify and review the image. Opp. at Ex. A p. 3. Instead, PhotoDNA identified the image, which “Microsoft’s human review ... confirmed ... was child sexual exploitation and abuse imagery, classified as A1...” *Id.* But Microsoft made clear it “conducts human review of every image PhotoDNA flags or has flagged to confirm the image is CSEAI.” *Id.* at Ex. A p. 6. And as Microsoft also explained, it does not record who reviews which PhotoDNA-flagged image to protect the safety of its content analysts, including in the event of a subsequent criminal investigation. *Id.*

(b) ensured the image that PhotoDNA flagged in Claimant's OneDrive had been confirmed by a Microsoft content analyst to be CSEAI and therefore objectionable to Microsoft and in violation of the Code of Conduct; and (c) as a result, blocked Claimant's OneDrive. Mot. at 6-8; Microsoft's Opp. to Mtn. to Compel, p. 8; Opp. at Ex. A p. 3 ("Microsoft's human review has confirmed that this same image was child sexual exploitation and abuse imagery, classified as A1 (the most egregious form of this material)."). That Microsoft blocked Claimant's entire OneDrive, not just the image, cannot demonstrate bad faith as a matter of law. Indeed, the Second Circuit in *Vimeo* rejected this very argument, confirming that Section 230 "does not require providers to use any particular form of restriction" and affirming Vimeo's decision there to block the user's entire account. Mot. at 12-13 (citing and discussing *Vimeo*, 991 F.3d at 72). The Arbitrator should grant Microsoft's Motion under Section 230 and should dismiss Claimant's Third and Fourth Amended Demands.

The Arbitrator should also dismiss Claimant's Windows 10 claim on this basis. Claimant rests this claim on the fact Microsoft blocked his OneDrive upon detecting content Microsoft considers objectionable in the account (CSEAI), allegedly preventing him from backing up his content once Windows 10 allegedly failed. See Fourth Amended Demand at 2-3, 8-9 (Windows 10 allegations). To allow Claimant to continue litigating this claim despite Microsoft's immunity for its blocking action would effectively allow him to make an end-run around Section 230.

d. The Arbitrator Should Dismiss the Fourth Amended Demand Without Leave to Amend a Fifth Time.

Claimant filed his initial arbitration demand nearly a year ago, in August 2020. Since that time, this matter has involved a motion for emergent relief, three iterations of the arbitration demand, one round of discovery, and various issues requiring arbitral intervention. This consumer arbitration should have reached an expedient and efficient resolution long ago.

From the time of Microsoft's first appearance in this case, Claimant has been on notice that Microsoft seeks immunity under Section 230 of the Communications Decency Act. Microsoft set forth its analysis of the statute in its opposition to Claimant's motion for emergent relief, after which Claimant was permitted to amend his demand and obtain discovery. After that, he had yet another opportunity to amend the Demand in an effort to allege facts showing lack of good faith under Section 230. Claimant still has not alleged such facts despite four amendments and discovery, revealing that any further amendment would be futile and would serve only to circumvent the statute's objective of avoiding providers "having to fight costly and protracted legal battles." *Nemet Chevrolet, Ltd. v. Consumeraffairs.com, Inc.*, 591 F.3d 250, 255 (4th Cir.

2009).

III. CONCLUSION

For the reasons set forth above and in Microsoft's Motion for Judgment on the Pleadings, Microsoft respectfully requests that the Arbitrator dismiss Claimant's Third and Fourth Amended Demands with prejudice under Section 230(c)(2)(A).

Dated: June 18, 2021

RESPONDENT MICROSOFT CORPORATION

By: /s/ Natalie Nahabet
Marc R. Shapiro (NY SBN 4403606)
Natalie Nahabet (CA SBN 301597)
ORRICK, HERRINGTON & SUTCLIFFE LLP
777 South Figueroa Street, Suite 3200
Los Angeles, CA 90017
Telephone: (213) 629-2020
Facsimile: (213) 612-2499
Email: mrshapiro@orrick.com
nnahabet@orrick.com

ATTORNEYS FOR RESPONDENT MICROSOFT
CORPORATION

EXHIBIT 25

From: Harriet Derman <hderman@newjerseylaw.net>
Sent: Thursday, June 24, 2021 7:56 AM
To: AAA Jenna Pascale
Cc: Nahabet, Natalie; Jason Lampert; bwilliamson@slwlawoffices.com; Shapiro, Marc R.; Efthimios Parasidis; cc: Frank Salzano
Subject: Re: Thomas Deutsch, Esq. v. Microsoft Corporation - Case 01-20-0014-3715

Dear Counsel,

I am asking Microsoft to address by tomorrow morning Claimant's claims for negligence and breach of contract with respect to the allegedly defective software problem. Claimant may respond by the end of the day tomorrow. Judge Derman

On Thu, Jun 24, 2021 at 10:46 AM <jennapascale@adr.org> wrote:

Hello,

Please review the attached correspondence regarding the above-referenced case.

Feel free to contact me with any questions, comments or concerns you have related to this matter.

Thank you.

[Logo]

AAA Jenna Pascale
Case Administrator
American Arbitration Association

1301 Atwood Ave, Suite 211N, Johnston, RI 02919

T: 401 406 7095

[adr.org](https://www.adr.org)<<https://www.adr.org>> | [icdr.org](https://www.icdr.org)<<https://www.icdr.org>> | [aaamediation.org](https://www.aaamediation.org)<<https://www.aaamediation.org>>

Adam Shoneck, Assistant Vice President
Northeast Case Management Center
[cid:image5f3ed8.PNG@fa18daca.4cb6e7f3]

The information in this transmittal (including attachments, if any) is privileged and/or confidential and is intended only for the recipient(s) listed above. Any review, use, disclosure, distribution or copying of this transmittal is prohibited

except by or on behalf of the intended recipient. If you have received this transmittal in error, please notify me immediately by reply email and destroy all copies of the transmittal. Thank you.

EXHIBIT 26

From: Nahabet, Natalie
Sent: Friday, August 20, 2021 2:19 PM
To: Harriet Derman; Shapiro, Marc R.
Cc: Efthimios Parasidis; Jason Lampert; Frank Salzano; Brady Williamson
Subject: RE: Windows 10 Briefing Schedule
Attachments: Proposed Order Granting Motion for Judgment on the Pleadings.docx

Judge Derman,

Please see attached for the proposed order on the motion for judgment on the pleadings and motion to compel, which tracks your oral ruling.

Hope you have a great weekend!

Sincerely,
Natalie

Natalie Nahabet
Orrick | 213-612-2324

From: Harriet Derman <hderman@newjerseylaw.net>
Sent: Thursday, August 19, 2021 5:56 AM
To: Shapiro, Marc R. <mrshapiro@orrick.com>
Cc: Nahabet, Natalie <nnahabet@orrick.com>; Efthimios Parasidis <eparasidis@slwlawoffices.com>; Jason Lampert <jlampert@slwlawoffices.com>; Frank Salzano <fsalzano@slwlawoffices.com>; Brady Williamson <bwilliamson@slwlawoffices.com>
Subject: Re: Windows 10 Briefing Schedule

That schedule is acceptable. Thank you. Harriet Derman

On Wed, Aug 18, 2021 at 7:42 PM Shapiro, Marc R. <mrshapiro@orrick.com> wrote:

Judge Derman:

The parties have agreed to the following briefing schedule on the outstanding Windows 10 claims:


Sept. 10: Microsoft's opening brief due.

Oct. 4: Claimant's opposition due.

Oct. 15: Microsoft's reply brief due.

Regards,
Marc Shapiro

Marc Shapiro
Attorney at Law

Orrick
New York 
T +1-212-506-3546
mrshapiro@orrick.com



NOTICE TO RECIPIENT | This e-mail is meant for only the intended recipient of the transmission, and may be a communication privileged by law. If you received this e-mail in error, any review, use, dissemination, distribution, or copying of this e-mail is strictly prohibited. Please notify us immediately of the error by return e-mail and please delete this message from your system. Thank you in advance for your cooperation.

For more information about Orrick, please visit <http://www.orrick.com>.

In the course of our business relationship, we may collect, store and transfer information about you. Please see our privacy policy at <https://www.orrick.com/Privacy-Policy> to learn about how we use this information.

AMERICAN ARBITRATION ASSOCIATION

THOMAS DEUTSCH, ESQ.,	:	
	:	
<i>Claimant,</i>	:	CASE NO. 01-20-0014-3715
	:	
v.	:	
	:	
MICROSOFT CORPORATION,	:	
	:	
<i>Respondent.</i>	:	

**ORDER GRANTING RESPONDENT’S MOTION FOR JUDGMENT ON THE
PLEADINGS AND DENYING CLAIMANT’S MOTION TO COMPEL**

Having considered the parties’ briefs, supporting documentation, and arguments, it is hereby ordered that Respondent’s Motion for Judgment on the Pleadings is GRANTED based on the following:

1. Section 230(c)(2)(A) of the Communications Decency act states: “No provider or user of an interactive computer service shall be held liable on account of -- (A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected....” 47 U.S.C. § 230(c)(2)(A).

2. Section 230 has been interpreted expansively and its purpose is to allow providers to police content without being concerned over the legal ramifications. As stated in Section 230(b), it is the policy of the United States “to remove disincentives for the development and utilization of blocking and filtering technologies...” and “to ensure vigorous enforcement of Federal criminal laws to deter and punish trafficking in obscenity, stalking, and harassment by means of computer.” *Id.* at § 230(b)(4)-(5). The purpose of Section 230(c)(2) is to provide platforms with the discretion to identify and remove what they consider objectionable without incurring liability for each decision. *See, e.g., Domen v. Vimeo*, -- F. 4th --, 2021 U.S. App. LEXIS 21533 (2d Cir. July 21, 2021).

3. Congress intended for Section 230 to provide not just immunity from liability, but from suit. *See, e.g., Obado v. Magedson*, 612 Fed. Appx. 90, 93 (3d Cir. 2015). Section 230 is thus intended to allow providers to avoid litigation in the first instance. Moreover, it is clear that Congress wanted to eliminate pornography from the internet and did not want companies to be sued by allowing companies to take action even when objectionable content is simply stored, with the potential to share, even though the individual did not yet share, but had the opportunity to do so.

4. Here, Claimant agreed to the Microsoft Services Agreement (“MSA”), which contains the Code of Conduct, and is very clear as to what will be tolerated on the Microsoft platform, as well as the ramifications if there is a breach. Section 3(a)(ii) of the MSA states that a user shall not “engage in any activity that exploits, harms, or threatens to harm children.” Section 3(b) states, “If you violate these Terms, we may stop providing Services to you or we may close your Microsoft account.” Microsoft therefore warns users that their accounts may be suspended if they breach the MSA. Claimant may not have believed that this would happen to him, but he nevertheless agreed to these terms.

5. Microsoft’s Privacy Statement, which Claimant also agreed to, informs users that Microsoft reserves the right to scan user’s files. It states, “some of our products, such as Outlook or OneDrive, systematically scan content in an automated manner to identify suspected spam, viruses, [and] abusive actions...” Privacy Statement at 8. It further states that Microsoft “will retain, access, transfer, disclose, and preserve personal data, including your content (such as the content of your emails in Outlook.com, or files in private folders on OneDrive), when we have a good faith belief that doing so is necessary to do any of the following: ... Protect the rights or property of Microsoft, including enforcing the terms governing the use of the services...”

6. In May 2020, Microsoft suspended Claimant’s OneDrive account after identifying an image it considered to be child sexual exploitation and abuse imagery (“CSEAI”) within the account and thus violative of Microsoft’s content policies under the MSA. Claimant disputes that the image is CSEAI, and the image has not been verified to be CSEAI.

7. In summary, Microsoft argues in its Motion for Judgment on the Pleadings that it acted within the scope of the protections offered by Section 230 where its actions were taken in good faith. Claimant argues that Section 230 limitations do not cover Microsoft’s conduct, that OneDrive is not an interactive computer service, and that Microsoft acted in bad faith.

8. A motion for judgment on the pleadings is evaluated under the same standard as that for failure to state a claim. *Wolfington v. Reconstructive Orthopedic Assoc. II PC*, 935 F.3d

187, 195 (3d Cir. 2019). When considering a motion for judgment on the pleadings, the court asks whether the non-moving party is entitled to provide evidence to support the claim. *Rodriguez v. City of Camden*, 2010 WL 186248, at *2 (D.N.J. Jan. 13, 2010). A cause of action must be dismissed if the claimant fails to articulate a legal basis entitling him to relief. Moreover, the “court may consider documents specifically referenced in the complaint ‘without converting the motion into one for summary judgment.’” *Norcross v. Murphy*, 2020 WL 3634750, at *6 (N.J. App. Div. July 6, 2020) (citing *Banco Popular N. Am. V. Gandi*, 184 N.J. 161, 183 (2005)). Although plaintiffs are generally entitled to every reasonable inference of fact, “they may not rely on conclusory allegations, hoping that discovery will allow them to find that a cause of action exists.” *Id.* (citing *Printing Mart-Morristown v. Sharp Elecs. Corp.*, 116 N.J. 739, 768 (1989) (“A plaintiff can bolster a ... cause of action through discovery, but not [] file a conclusory complaint to find out if one exists.”) (internal quotations and citations omitted)).

9. Microsoft’s actions fall within the statutory purpose of Section 230 of the Communications Decency Act and it is entitled to immunity under the statute.

10. OneDrive is an “interactive computer service,” which is defined under the statute as “any information, service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the internet.” 47 U.S.C. § 230(f)(2). Furthermore, OneDrive is an “access software provider,” which is “a provider of software (including client or server software), or enabling tools that do any one or more of the following...(A) filter, screen, allow or disallow content; or ... (C) transmit, receive, display, forward, cache, search, subset, organize, reorganize, or translate content.” *Id.* at § 230(f)(4).

11. OneDrive is not just a “document storage system,” as Claimant suggests. OneDrive is a cloud computing service that provides users with online access to a cloud server on which users can store as well as share published content. It allows users to store files and access them from any device anywhere, share files with friends and family, and more. *See also* Privacy Statement at 34. OneDrive provides access by multiple users to a computer server. Companies are not excluded under the statute, which is to be construed expansively, for storage of content in private folders. Claimant admits that he used OneDrive to transmit his files to the cloud and to reorganize his files, as well as to continue to add to and modify his documents and data. Nor does Claimant cite to any authority that OneDrive falls outside the definition of an interactive computer service based on how the user chose to use the services in the particular case before the court. Nor would such a rule be workable. All that would be required is access to a computer server by

multiple users. Even if the statute limited an interactive computer service, Claimant's own pleadings confirm that he did use OneDrive to store and share content.

12. Moreover, Microsoft has acted in good faith here. Microsoft did not act with an anticompetitive intent, did not act on malicious whim, or act contrary to industry standard, and it did not target Claimant. Microsoft, through the industry-leading computer technology, PhotoDNA, which Microsoft uses to monitor images for CSEAI and to flag images it considers to be CSEAI, identified the image at issue here. Images flagged by PhotoDNA are subject to human review, where a Microsoft employee confirms the image is CSEAI. If an image has been confirmed to be CSEAI, Microsoft removes the Image and suspends the account. The flagged image went through this process. While Claimant argues human review has not been done because Microsoft cannot name any individual who has reviewed the image in its interrogatory response, Microsoft denies this and states in its response that it does not maintain a record of the individual to protect the analysts who conduct this review and make such determinations.

13. Sean Davis had stated that PhotoDNA scans images that are shared or made public and that Microsoft does not search private images. This statement was retracted after Microsoft learned the image at issue here was not shared via OneDrive and Microsoft promptly disclosed this fact to Claimant and the tribunal. While the statement is problematic, it does not require the imposition of liability because it reflects an "imperfect exercise of content-policing" and does not demonstrate bad faith. *Domen v. Vimeo*, 2021 U.S. App. LEXIS 21533 at *17. Additionally, the statement is only evidence that Microsoft violated its own internal policies but all actions were otherwise taken in accordance with the MSA and Privacy Statement. Moreover, the fact that the image was not shared through OneDrive does not impact Microsoft's immunity where the definition of an interactive computer service does not turn on shared content. Nor does Claimant cite to any authority in support of his argument that Section 230 should not apply because the image was not shared. *See, e.g., Holomaxx Techs. v. Yahoo!, Inc.*, 2011 WL 3740827, at *2 (N.D. Cal. Aug. 23, 2011) (holding Yahoo!'s blocking of spam was a covered action); *Holomaxx Techs. v. Microsoft Corp.*, 783 F. Supp. 2d 1097, 1104 (N.D. Cal. 2011) (holding Microsoft's blocking of marketing emails was a covered action); *Domen v. Vimeo*, 2021 U.S. App. LEXIS 21533 (upholding district court's Rule 12(b)(6) dismissal under Section 230(c)(2)(A) not because the user had shared the content with others on Vimeo, but because Vimeo subjectively believed the content was objectionable and in violation of its terms of use).

14. Mistakes made by Respondent are not enough to constitute bad faith. *See e360Insights, LLC v. Comcast Corp.*, 546 F. Supp. 2d 605, 609 (N.D. Ill. 2008); *NetChoice, LLC*

v. Moody, -- F.3d --, 2021 U.S. Dist. LEXIS 121951, at *19 (N.D. Fla. June 30, 2021). Even if Microsoft made a mistake, Section 230 affords it immunity from suit because Congress wanted providers to police their platform. Nonetheless, Section 230 provides subjective discretion to Microsoft in identifying images that it considers objectionable. Though the Second Circuit in *Domen v. Vimeo* originally stated that providers have “substantial subjective discretion,” 991 F.3d 66, 72 (2d Cir. 2021), in its now amended opinion it still recognizes that providers are “grant[ed] some degree of subjective discretion.” *Domen v. Vimeo*, 2021 U.S. App. LEXIS 21533 at *13 (“[T]he provision explicitly provides protection from suit for restricting access to content that providers ‘consider[] ... otherwise objectionable,’ even if the material would otherwise be constitutionally protected, granting some degree of subjective discretion to service providers who restrict the availability of content in good faith.”) (citing 47 U.S.C. § 230(c)(2) (emphasis in original)). As stated in *Smith v. Trusted Universal Standards in Elec. Transactions, Inc.*, “Section 230(c)(2)(A) does not require the user or provider of an interactive computer service to demonstrate that the otherwise ‘objectionable’ material is actually objectionable.” 2011 WL 900096 (D.N.J. Mar. 15, 2011) (citing *Zango, Inc. v. Kaspersky Lab, Inc.*, 2007 WL 5189857 at *4 (W.D. Wash. Aug. 28, 2007)). For example, defendants in *Trusted Universal* had the latitude or discretion as to what they considered to be spam under the statute, and the court found two of the three defendants there immune. *Id.*

15. While Claimant has cited to numerous cases, he does not cite to cases addressing the relevant statute. Claimant refers to cases addressing Section 230(c)(1) and published or shared content. However, Microsoft moves under Section 230(c)(2), not (c)(1).

16. Rule 33 of the Consumer Rules of the American Arbitration Association provide an arbitrator with authority to dispose of a case at this point in the proceedings. While often amendment of complaints are allowed in the interest of justice, a court can deny leave to amend when the moving party has shown to this tribunal that amendment would be futile, which would be the case here. *Bailey v. U.S. Marshals Service Headquarters*, 426 Fed. Appx. 44 (3d Cir. 2011) (“Leave to amend a complaint is futile when the complaint as amended would still be properly dismissed or be immediately subject to summary judgment for the defendant.”) (citations and internal quotations omitted). *See also Wolfington*, 935 F.3d at 195. Claimant is denied an opportunity to amend his complaint for the fifth time, particularly where he submitted his fourth amended claim after having had the benefit of Respondent’s motion for judgment on the pleadings.

17. Claimant's breach of contract claims, with the exception of Section F of Count 2 of the Fourth Amended Claim (Windows 10 Breach of EULA), are hereby dismissed. *See Trusted Universal*, 2011 WL 900096, at *8.

18. Claimant's breach of the implied covenant of good faith and fair dealing claims are hereby dismissed. *See Federal Agency of News LLC v. Facebook, Inc.*, 432 F. Supp. 3d 1107, 1120 (N.D. Cal. 2020).

19. Claimant's negligence claims, with the exception of Section E of Count 4 of the Fourth Amended Claim (Windows 10 Negligence), are hereby dismissed. *See Riggs v. Myspace, Inc.*, 2011 WL 3020543, at *1 (9th Cir. July 25, 2011).

20. Claimant's breach of privacy claims are hereby dismissed. *See Poole v. Tumblr, Inc.*, 404 F. Supp. 3d 637, 643 (D. Conn. 2019).

21. Claimant's conversion claims are hereby dismissed. *See Franklin v. X Gear 101, LLC*, 2018 WL 4103492, at *8 (S.D.N.Y. Aug. 28, 2018).

22. Claimant's consumer fraud claims are hereby dismissed. *See e360 Insights*, 546 F. Supp. 2d 605.

In light of the Arbitrator's dismissal of all claims pertaining to Claimant's OneDrive account, it is hereby ordered that Claimant's motion to compel Microsoft to produce the image that resulted in his OneDrive account being suspended is DENIED as moot.

Therefore, it is hereby ordered that Respondent's Motion for the Judgment on the Pleadings is GRANTED without leave to amend and Claimant's Motion to Compel is hereby DENIED. The Parties shall submit briefing to address the remaining Windows 10 claims of breach of contract and negligence.

Dated: August __, 2021

THE HONORABLE HARRIET DERMAN, J.S.C.
(Ret), Arbitrator

By: _____

EXHIBIT 27

AMERICAN ARBITRATION ASSOCIATION

THOMAS DEUTSCH, ESQ.,

Claimant,

v.

MICROSOFT CORPORATION,

Respondent.:
:
:
:
:
:
:
:
:
:

CASE NO. 01-20-0014-3715

ORDER GRANTING RESPONDENT'S MOTION FOR JUDGMENT ON A PORTION OF THE PLEADINGS AND DENYING CLAIMANT'S MOTION TO COMPEL

Having considered the parties' briefs, supporting documentation, and arguments on August 18, 2021, it is hereby ordered that Respondent's Motion for Judgment on the Pleadings is GRANTED in part and denied in part based on the following:

1. As explained hereafter, Microsoft's actions were within the scope of Section 230's statutory purpose; OneDrive is an "interactive computer service"; and Microsoft acted in good faith.

2. Section 230(c)(2)(A) of the Communications Decency act states: "No provider or user of an interactive computer service shall be held liable on account of -- (A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected...." 47 U.S.C. § 230(c)(2)(A).

3. Section 230 has been interpreted expansively and its purpose is to allow providers to police content without being concerned over the legal ramifications. As stated in Section 230(b), it is the policy of the United States "to remove disincentives for the development and utilization of blocking and filtering technologies..." and "to ensure vigorous enforcement of Federal criminal laws to deter and punish trafficking in obscenity, stalking, and harassment by means of computer." *Id.* at § 230(b)(4)-(5). The purpose of Section 230(c)(2) is to provide platforms with the discretion to identify and remove what they consider objectionable without

incurring liability for each decision. *See, e.g., Domen v. Vimeo*, -- F. 4th --, 2021 U.S. App. LEXIS 21533 (2d Cir. July 21, 2021).

4. Congress intended Section 230 to provide not just immunity from liability, but from suit. *See, e.g., Obado v. Magedson*, 612 Fed. Appx. 90, 93 (3d Cir. 2015). Section 230 is thus intended to allow providers to avoid litigation in the first instance. Moreover, it is clear that Congress wanted to eliminate pornography from the internet. It did not want providers to be sued by allowing companies to act even when objectionable content is simply stored, with the potential to share, and even though the individual did not yet share, but had the opportunity to do so.

5. Here, Claimant agreed to the Microsoft Services Agreement (“MSA”), which contains the Code of Conduct, and it is very clear as to what will be tolerated on the Microsoft platform, as well as the ramifications if there is a breach. Section 3(a)(ii) of the MSA states that a user shall not “engage in any activity that exploits, harms, or threatens to harm children.” Section 3(b) states, “If you violate these Terms, we may stop providing Services to you or we may close your Microsoft account.” Microsoft therefore warns users, including Claimant, that their accounts may be suspended if they breach the MSA. Claimant may not have believed that this would happen to him, but he nevertheless agreed to these terms.

6. Microsoft’s Privacy Statement, to which Claimant also agreed, informs users that Microsoft reserves the right to scan user’s files. It states, “some of our products, such as Outlook or OneDrive, systematically scan content in an automated manner to identify suspected spam, viruses, [and] abusive actions....” Privacy Statement at 8. It further states that Microsoft “will retain, access, transfer, disclose, and preserve personal data, including your content (such as the content of your emails in Outlook.com, or files in private folders on OneDrive), when we have a good faith belief that doing so is necessary to do any of the following: ... Protect the rights or property of Microsoft, including enforcing the terms governing the use of the services....”

7. In May 2020, Microsoft suspended Claimant’s OneDrive account after identifying an image it considered to be child sexual exploitation and abuse imagery (“CSEAI”) within the account and thus violative of Microsoft’s content policies under the MSA. Claimant disputes that the image is CSEAI and claims the image has not been verified to be CSEAI.

8. In summary, Microsoft argues in its Motion for Judgment on the Pleadings that it acted within the scope of the protections offered by Section 230 because its actions were taken in good faith. Claimant argues that Section 230 limitations do not cover Microsoft’s conduct, that OneDrive is not an interactive computer service, and that Microsoft acted in bad faith.

9. A motion for judgment on the pleadings is evaluated under the same standard as failure to state a claim upon which relief can be granted. *Wolffington v. Reconstructive Orthopedic Assoc. II PC*, 935 F.3d 187, 195 (3d Cir. 2019). When considering a motion for judgment on the pleadings, the court asks whether the non-moving party is entitled to provide evidence to support the claim. *Rodriguez v. City of Camden*, 2010 WL 186248, at *2 (D.N.J. Jan. 13, 2010). A cause of action must be dismissed if the claimant fails to articulate a legal basis entitling him to relief. Moreover, the “court may consider documents specifically referenced in the complaint ‘without converting the motion into one for summary judgment.’” *Norcross v. Murphy*, 2020 WL 3634750, at *6 (N.J. App. Div. July 6, 2020) (citing *Banco Popular N. Am. V. Gandi*, 184 N.J. 161, 183 (2005)). Although plaintiffs are generally entitled to every reasonable inference of fact, “they may not rely on conclusory allegations, hoping that discovery will allow them to find that a cause of action exists.” *Id.* (citing *Printing Mart-Morristown v. Sharp Elecs. Corp.*, 116 N.J. 739, 768 (1989) (“A plaintiff can bolster a ... cause of action through discovery, but not [] file a conclusory complaint to find out if one exists.”) (internal quotations and citations omitted)).

10. Rule 33 of the Consumer Rules of the American Arbitration Association provides an arbitrator with authority to dispose of a case at this point in the proceedings.

11. Microsoft’s actions fall within the statutory purpose of Section 230 of the Communications Decency Act and it is entitled to immunity under the statute.

12. OneDrive is an “interactive computer service,” which is defined under the statute as “any information, service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the internet.” 47 U.S.C. § 230(f)(2). Furthermore, OneDrive is an “access software provider,” which is “a provider of software (including client or server software), or enabling tools that do any one or more of the following...(A) filter, screen, allow or disallow content; or ... (C) transmit, receive, display, forward, cache, search, subset, organize, reorganize, or translate content.” *Id.* at § 230(f)(4).

13. Courts interpret “interactive computer service” broadly. *See Poole v. Tumblr, Inc.*, 404 F. Supp. 3d 637, 641 (D. Conn. 2019)(noting that Section 230 defines the term “extensively in order to effectuate the statute’s speech-protective purpose”); *Smith v. Trusted Universal Standards Elec. Transactions, Inc.*, No. 09-4567, 2011 WL 900096, at *4 (D.N.J. Mar. 15, 2011) (“courts generally construe the terms ‘interactive computers service’ very broadly”).

14. OneDrive is not just a “document storage system,” as Claimant suggests. OneDrive is a cloud computing service that provides users with online access to a cloud server on which

users can store as well as share published content. It allows users to store files and access them from any device anywhere, share files with friends and family, and more. *See also* Privacy Statement at 34. OneDrive provides access by multiple users to a computer server. Companies are not excluded under the statute, which is to be construed expansively, for storage of content in private folders. Claimant admits that he used OneDrive to transmit his files to the cloud and to reorganize his files, as well as to continue to add to and modify his documents and data. Nor does Claimant cite to any authority that OneDrive falls outside the definition of an interactive computer service based on how the user chose to use the services in the particular case before the court. Nor would such a rule be workable. All that would be required is access to a computer server by multiple users. Even if the statute limited an interactive computer service, Claimant's own pleadings confirm that he did use OneDrive to store and share content.

15. Sean Davis, head of Digital Safety Operations at Microsoft, had stated in his affidavit that PhotoDNA scans images that are shared or made public and that Microsoft does not search private images. This statement was promptly retracted after Microsoft learned the image at issue here was not shared via OneDrive and Microsoft promptly disclosed this fact to Claimant and the tribunal. While the statement is problematic, it does not require the imposition of liability because it reflects an "imperfect exercise of content-policing" and does not demonstrate bad faith. *Domen v. Vimeo*, 2021 U.S. App. LEXIS 21533 at *17. Additionally, the statement is only evidence that Microsoft violated its own internal policies but all actions were otherwise taken in accordance with the MSA and Privacy Statement.

16. Moreover, the fact that the image was not shared through OneDrive does not impact Microsoft's immunity where the definition of an interactive computer service does not turn on shared content. Nor does Claimant cite to any authority in support of his argument that Section 230 should not apply because the image was not shared. *See, e.g., Holomaxx Techs. v. Yahoo!, Inc.*, 2011 WL 3740827, at *2 (N.D. Cal. Aug. 23, 2011) (holding Yahoo!'s blocking of spam was a covered action); *Holomaxx Techs. v. Microsoft Corp.*, 783 F. Supp. 2d 1097, 1104 (N.D. Cal. 2011) (holding Microsoft's blocking of marketing emails was a covered action); *Domen v. Vimeo*, 2021 U.S. App. LEXIS 21533 (upholding district court's Rule 12(b)(6) dismissal under Section 230(c)(2)(A) not because the user had shared the content with others on Vimeo, but because Vimeo subjectively believed the content was objectionable and in violation of its terms of use).

17. Moreover, Microsoft has acted in good faith here. Microsoft did not act with an anticompetitive intent, did not act on malicious whim, or act contrary to industry standard, and it did not target Claimant. Microsoft, through the industry-leading computer technology,

PhotoDNA, which Microsoft uses to monitor images for CSEAI and to flag images it considers to be CSEAI, identified the image at issue here. Images flagged by PhotoDNA are subject to human review where a Microsoft employee confirms the image is CSEAI. If an image has been confirmed to be CSEAI, Microsoft removes the Image and suspends the account. The flagged image went through this process. While Claimant argues human review has not been done because Microsoft cannot name any individual who has reviewed the image in its interrogatory response, Microsoft denies this and states in its response that it does not maintain a record of the individual to protect the analysts who conduct these reviews and make such determinations.

18. Mistakes made by Respondent are not enough to constitute bad faith. *See e360Insights, LLC v. Comcast Corp.*, 546 F. Supp. 2d 605, 609 (N.D. Ill. 2008); *NetChoice, LLC v. Moody*, -- F.3d --, 2021 U.S. Dist. LEXIS 121951, at *19 (N.D. Fla. June 30, 2021). Even if Microsoft made a mistake, Section 230 affords it immunity from suit because Congress wanted providers to police their platforms. Nonetheless, Section 230 provides subjective discretion to Microsoft in identifying images that it considers objectionable. Though the Second Circuit in *Domen v. Vimeo* originally stated that providers have “substantial subjective discretion,” 991 F.3d 66, 72 (2d Cir. 2021), in its now amended opinion it still recognizes that providers are “grant[ed] some degree of subjective discretion.” *Domen v. Vimeo*, 2021 U.S. App. LEXIS 21533 at *13 (“[T]he provision explicitly provides protection from suit for restricting access to content that providers ‘consider[] ... otherwise objectionable,’ even if the material would otherwise be constitutionally protected, granting some degree of subjective discretion to service providers who restrict the availability of content in good faith.”) (citing 47 U.S.C. § 230(c)(2) (emphasis in original)). As stated in *Smith v. Trusted Universal Standards in Elec. Transactions, Inc.*, “Section 230(c)(2)(A) does not require the user or provider of an interactive computer service to demonstrate that the otherwise ‘objectionable’ material is actually objectionable.” 2011 WL 900096 (D.N.J. Mar. 15, 2011) (citing *Zango, Inc. v. Kaspersky Lab, Inc.*, 2007 WL 5189857 at *4 (W.D. Wash. Aug. 28, 2007)). For example, defendants in *Trusted Universal* had the latitude or discretion as to what they considered to be spam under the statute, and the court found two of the three defendants immune from liability. *Id.*

19. While Claimant has cited to numerous cases, he does not cite to cases addressing the relevant statute. Claimant refers to cases addressing Section 230(c)(1) and its progeny dealing with published or shared content. Microsoft, however, moves under Section 230(c)(2), not (c)(1).

20. While often amendments of complaints are allowed in the interest of justice, a court can deny leave to amend when the moving party has shown to the tribunal that amendment

would be futile, which would be the case here. *Bailey v. U.S. Marshals Service Headquarters*, 426 Fed. Appx. 44 (3d Cir. 2011) (“Leave to amend a complaint is futile when the complaint as amended would still be properly dismissed or be immediately subject to summary judgment for the defendant.”) (citations and internal quotations omitted). *See also Wolfington*, 935 F.3d at 195. Claimant is denied an opportunity to amend his complaint for the fifth time, particularly where he submitted his fourth amended claim after having had the benefit of Respondent’s motion for judgment on the pleadings. “Indeed, a ‘district court’s discretion to deny leave to amend is particularly broad where plaintiff has previously amended the complaint.’” *In re Zoom Video Communications Inc. Privacy Litigation*, No.20-CV-02155-LHK, 2021 U.S. Dist. LEXIS 47095, at *23-26 (N.D. Cal. March 11, 2021) (citing *Cafasso, U.S. ex rel Gen. Dynamics C4 Sys., Inc.*, 637 F.3d 1047, 1058 (9th Cir. 2011)).

21. Claimant’s breach of contract claims, with the exception of Section F of Count 2 of the Fourth Amended Claim (Windows 10 Breach of EULA), are hereby dismissed. *See Trusted Universal*, 2011 WL 900096, at *8.

22. Claimant’s breach of the implied covenant of good faith and fair dealing claims are hereby dismissed. *See Federal Agency of News LLC v. Facebook, Inc.*, 432 F. Supp. 3d 1107, 1120 (N.D. Cal. 2020).

23. Claimant’s negligence claims, with the exception of Section E of Count 4 of the Fourth Amended Claim (Windows 10 Negligence), are hereby dismissed. *See Riggs v. Myspace, Inc.*, 2011 WL 3020543, at *1 (9th Cir. July 25, 2011).

24. Claimant’s breach of privacy claims are hereby dismissed. *See Poole v. Tumblr, Inc.*, 404 F. Supp. 3d 637, 643 (D. Conn. 2019).

25. Claimant’s conversion claims are hereby dismissed. *See Franklin v. X Gear 101, LLC*, 2018 WL 4103492, at *8 (S.D.N.Y. Aug. 28, 2018).

26. Claimant’s consumer fraud claims are hereby dismissed. *See e360 Insights*, 546 F. Supp. 2d 605 (N. D. Ill 2008); *In re Zoom Video Communications Inc. Privacy Litigation*, 2021 U.S. Dist. LEXIS 47095, at *65-66.

In light of the Arbitrator’s dismissal of all claims pertaining to Claimant’s OneDrive account, it is hereby ordered that Claimant’s motion to compel Microsoft to produce the image that resulted in his OneDrive account being suspended is DENIED as moot.

Therefore it is hereby ordered that Respondent’s Motion for the Judgment on a portion of the Pleadings is GRANTED without leave to amend and Claimant’s Motion to Compel is hereby

DENIED. The Parties shall submit briefing to address the remaining Windows 10 claims of breach of contract and negligence.

Dated: August 23, 2021

THE HONORABLE HARRIET DERMAN, J.S.C.
(Ret), Arbitrator

A handwritten signature in cursive script that reads "Harriet Derman". The signature is written in dark ink and is positioned above a horizontal line.

By: _____

EXHIBIT 27A

AMERICAN ARBITRATION ASSOCIATION

THOMAS DEUTSCH, ESQ.,

=

Claimant,

v.

MICROSOFT CORPORATION,

Respondent.

:

=

:

=

:

=

:

=

:

=

:

÷

÷

÷

=

•

•

•

•

•

CASE NO. 01-20-0014-3715

ORDER GRANTING RESPONDENT'S MOTION FOR JUDGMENT ON [A PORTION](#)
[OF](#) THE PLEADINGS AND DENYING CLAIMANT'S MOTION TO COMPEL

Having considered the parties' briefs, supporting documentation, and arguments on August 18, 2021, it is hereby ordered that Respondent's Motion for Judgment on the Pleadings is GRANTED in part and denied in part based on the following:

1. As explained hereafter, Microsoft's actions were within the scope of Section 230's statutory purpose; OneDrive is an "interactive computer service"; and Microsoft acted in good faith.

2. ~~1.~~ Section 230(c)(2)(A) of the Communications Decency act states: "No provider or user of an interactive computer service shall be held liable on account of -- (A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected~~...~~." 47 U.S.C.

§ 230(c)(2)(A).

3. ~~2.~~ Section 230 has been interpreted expansively and its purpose is to allow providers to police content without being concerned over the legal ramifications. As stated in Section 230(b), it is the policy of the United States "to remove disincentives for the development and utilization of blocking and filtering technologies~~...~~" and "to ensure vigorous enforcement of Federal criminal laws to deter and punish trafficking in obscenity, stalking, and harassment by means of computer." *Id.* at § 230(b)(4)-(5). The purpose of Section 230(c)(2) is to provide platforms with the discretion to identify and remove what they consider objectionable without

incurring liability for each decision. *See, e.g., Domen v. Vimeo*, -- F. 4th --, 2021 U.S. App. LEXIS 21533 (2d Cir. July 21, 2021).

0. ~~3.~~ Congress intended ~~for~~ Section 230 to provide not just immunity from liability, but from suit. *See, e.g., Obado v. Magedson*, 612 Fed. Appx. 90, 93 (3d Cir. 2015). Section 230 is thus intended to allow providers to avoid litigation in the first instance. Moreover, it is clear that Congress wanted to eliminate pornography from the internet ~~and~~. It did not want ~~companies~~ providers to be sued by allowing companies to ~~take action~~ act even when objectionable content is simply stored, with the potential to share, and even though the individual did not yet share, but had the opportunity to do so.

1. ~~4.~~ Here, Claimant agreed to the Microsoft Services Agreement (“MSA”), which contains the Code of Conduct, and it is very clear as to what will be tolerated on the Microsoft platform, as well as the ramifications if there is a breach. Section 3(a)(ii) of the MSA states that a user shall not “engage in any activity that exploits, harms, or threatens to harm children.” Section 3(b) states, “If you violate these Terms, we may stop providing Services to you or we may close your Microsoft account.” Microsoft therefore warns users, including Claimant, that their accounts may be suspended if they breach the MSA. Claimant may not have believed that this would happen to him, but he nevertheless agreed to these terms.

2. ~~5.~~ Microsoft’s Privacy Statement, to which Claimant also agreed ~~to~~, informs users that Microsoft reserves the right to scan user’s files. It states, “some of our products, such as Outlook or OneDrive, systematically scan content in an automated manner to identify suspected spam, viruses, [and] abusive actions~~---~~.” Privacy Statement at 8. It further states that Microsoft “will retain, access, transfer, disclose, and preserve personal data, including your content (such as the content of your emails in ~~Outlook.com~~ Outlook.com, or files in private folders on OneDrive), when we have a good faith belief that doing so is necessary to do any of the following: ~~---~~.” Protect the rights or property of Microsoft, including enforcing the terms governing the use of the services~~---~~.”

3. ~~6.~~ In May 2020, Microsoft suspended Claimant’s OneDrive account after identifying an image it considered to be child sexual exploitation and abuse imagery (“CSEAI”) within the account and thus violative of Microsoft’s content policies under the MSA. Claimant disputes that the image is CSEAI, and claims the image has not been verified to be CSEAI.

4. ~~7.~~ In summary, Microsoft argues in its Motion for Judgment on the Pleadings that it acted within the scope of the protections offered by Section 230 ~~where~~ because its actions were

taken in good faith. Claimant argues that Section 230 limitations do not cover Microsoft's conduct, that OneDrive is not an interactive computer service, and that Microsoft acted in bad faith.

4. ~~8.~~ A motion for judgment on the pleadings is evaluated under the same standard as ~~that for~~ failure to state a claim upon which relief can be granted. *Wolfington v. Reconstructive Orthopedic Assoc. II PC*, 935 F.3d 187, 195 (3d Cir. 2019). When considering a motion for judgment on the pleadings, the court asks whether the non-moving party is entitled to provide evidence to support the claim. *Rodriguez v. City of Camden*, 2010 WL 186248, at *2 (D.N.J. Jan. 13, 2010). A cause of action must be dismissed if the claimant fails to articulate a legal basis entitling him to relief. Moreover, the “court may consider documents specifically referenced in the complaint ‘without converting the motion into one for summary judgment.’” *Norcross v. Murphy*, 2020 WL 3634750, at *6 (N.J. App. Div. July 6, 2020) (citing *Banco Popular N. Am. V. Gandi*, 184 N.J. 161, 183 (2005)). Although plaintiffs are generally entitled to every reasonable inference of fact, “they may not rely on conclusory allegations, hoping that discovery will allow them to find that a cause of action exists.” *Id.* (citing *Printing Mart-Morristown v. Sharp Elecs. Corp.*, 116 N.J. 739, 768 (1989) (“A plaintiff can bolster a ~~---~~ cause of action through discovery, but not [] file a conclusory complaint to find out if one exists.”)) (internal quotations and citations omitted).

5. Rule 33 of the Consumer Rules of the American Arbitration Association provides an arbitrator with authority to dispose of a case at this point in the proceedings.

6. ~~9.~~ Microsoft’s actions fall within the statutory purpose of Section 230 of the Communications Decency Act and it is entitled to immunity under the statute.

7. ~~10.~~ OneDrive is an “interactive computer service,” which is defined under the statute as “any information, service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the internet.” 47 U.S.C. § 230(f)(2). Furthermore, OneDrive is an “access software provider,” which is “a provider of software (including client or server software), or enabling tools that do any one or more of the following~~---~~ (A) filter, screen, allow or disallow content; or ~~---~~ (C) transmit, receive, display, forward, cache, search, subset, organize, reorganize, or translate content.” *Id.* at § 230(f)(4).

8. Courts interpret “interactive computer service” broadly. *See Poole v. Tumblr, Inc.*, 404 F. Supp. 3d 637, 641 (D. Conn. 2019) (noting that Section 230 defines the term “extensively in order to effectuate the statute’s speech-protective purpose”); *Smith v. Trusted Universal Standards Elec. Transactions, Inc.*, No. 09-4567, 2011 WL 900096, at *4 (D.N.J. Mar. 15, 2011) (“courts generally construe the terms ‘interactive computers service’ very broadly”).

9. ~~11.~~ OneDrive is not just a “document storage system,” as Claimant suggests.
OneDrive
is a cloud computing service that provides users with online access to a cloud server on which

3

users can store as well as share published content. It allows users to store files and access them from any device anywhere, share files with friends and family, and more. *See also* Privacy Statement at 34. OneDrive provides access by multiple users to a computer server. Companies are not excluded under the statute, which is to be construed expansively, for storage of content in private folders. Claimant admits that he used OneDrive to transmit his files to the cloud and to reorganize his files, as well as to continue to add to and modify his documents and data. Nor does Claimant cite to any authority that OneDrive falls outside the definition of an interactive computer service based on how the user chose to use the services in the particular case before the court. Nor would such a rule be workable. All that would be required is access to a computer server by multiple users. Even if the statute limited an interactive computer service, Claimant's own pleadings confirm that he did use OneDrive to store and share content.

~~12. Moreover, Microsoft has acted in good faith here. Microsoft did not act with an anticompetitive intent, did not act on malicious whim, or act contrary to industry standard, and it did not target Claimant. Microsoft, through the industry-leading computer technology, PhotoDNA, which Microsoft uses to monitor images for CSEAI and to flag images it considers to be CSEAI, identified the image at issue here. Images flagged by PhotoDNA are subject to human review, where a Microsoft employee confirms the image is CSEAI. If an image has been confirmed to be CSEAI, Microsoft removes the Image and suspends the account. The flagged image went through this process. While Claimant argues human review has not been done because Microsoft cannot name any individual who has reviewed the image in its interrogatory response, Microsoft denies this and states in its response that it does not maintain a record of the individual to protect the analysts who conduct this review and make such determinations.~~

10. ~~13.~~ Sean Davis, [head of Digital Safety Operations at Microsoft](#), had stated [in his affidavit](#) that PhotoDNA scans images that are shared or made public and that Microsoft does not search private images. This statement was [promptly](#) retracted after Microsoft learned the image at issue here was not shared via OneDrive and Microsoft promptly disclosed this fact to Claimant and the tribunal. While the statement is problematic, it does not require the imposition of liability because it reflects an "imperfect exercise of content-policing" and does not demonstrate bad faith. *Domen v. Vimeo*, 2021 U.S. App. LEXIS 21533 at *17. Additionally, the statement is only evidence that Microsoft violated its own internal policies but all actions were otherwise taken in accordance with the MSA and Privacy Statement.

11. Moreover, the fact that the image was not shared through OneDrive does not impact Microsoft's immunity where the definition of an interactive computer service does not turn on shared content. Nor does Claimant cite to any authority in support of his argument that Section 230 should not apply because the image was not shared. *See, e.g., Holomaxx Techs. v. Yahoo!, Inc.*, 2011 WL 3740827, at *2 (N.D. Cal. Aug. 23, 2011) (holding Yahoo!'s blocking of spam was a covered action); *Holomaxx Techs. v. Microsoft Corp.*, 783 F. Supp. 2d 1097, 1104 (N.D. Cal. 2011) (holding Microsoft's blocking of marketing emails was a covered action); *Domen v. Vimeo*, 2021 U.S. App. LEXIS 21533 (upholding district court's Rule 12(b)(6) dismissal under Section 230(c)(2)(A) not because the user had shared the content with others on Vimeo, but because Vimeo subjectively believed the content was objectionable and in violation of its terms of use).

12. Moreover, Microsoft has acted in good faith here. Microsoft did not act with an anticompetitive intent, did not act on malicious whim, or act contrary to industry standard, and it did not target Claimant. Microsoft, through the industry-leading computer technology.

PhotoDNA, which Microsoft uses to monitor images for CSEAI and to flag images it considers to be CSEAI, identified the image at issue here. Images flagged by PhotoDNA are subject to human review where a Microsoft employee confirms the image is CSEAI. If an image has been confirmed to be CSEAI, Microsoft removes the Image and suspends the account. The flagged image went through this process. While Claimant argues human review has not been done because Microsoft cannot name any individual who has reviewed the image in its interrogatory response, Microsoft denies this and states in its response that it does not maintain a record of the individual to protect the analysts who conduct these reviews and make such determinations.

5. ~~14.~~ Mistakes made by Respondent are not enough to constitute bad faith. See *e360Insights, LLC v. Comcast Corp.*, 546 F. Supp. 2d 605, 609 (N.D. Ill. 2008); *NetChoice, LLC v. Moody*, -- F.3d --, 2021 U.S. Dist. LEXIS 121951, at *19 (N.D. Fla. June 30, 2021). Even if Microsoft made a mistake, Section 230 affords it immunity from suit because Congress wanted providers to police their ~~platform~~platforms. Nonetheless, Section 230 provides subjective discretion to Microsoft in identifying images that it considers objectionable. Though the Second Circuit in *Domen v. Vimeo* originally stated that providers have “substantial subjective discretion,” 991 F.3d 66, 72 (2d Cir. 2021), in its now amended opinion it still recognizes that providers are “grant[ed] some degree of subjective discretion.” *Domen v. Vimeo*, 2021 U.S. App. LEXIS 21533 at *13 (“[T]he provision explicitly provides protection from suit for restricting access to content that providers ‘consider[] ~~---~~otherwise’ otherwise objectionable,” even if the material would otherwise be constitutionally protected, granting some degree of subjective discretion to service providers who restrict the availability of content in good faith.”) (citing 47 U.S.C. § 230(c)(2) (emphasis in original)). As stated in *Smith v. Trusted Universal Standards in Elec. Transactions, Inc.*, “Section 230(c)(2)(A) does not require the user or provider of an interactive computer service to demonstrate that the otherwise ‘objectionable’ material is actually objectionable.” 2011 WL 900096 (D.N.J. Mar. 15, 2011) (citing *Zango, Inc. v. Kaspersky Lab, Inc.*, 2007 WL 5189857 at *4 (W.D. Wash. Aug. 28, 2007)). For example, defendants in *Trusted Universal* had the latitude or discretion as to what they considered to be spam under the statute, and the court found two of the three defendants ~~there-immune~~from liability. *Id.*

6. ~~15.~~ While Claimant has cited to numerous cases, he does not cite to cases addressing the relevant statute. Claimant refers to cases addressing Section 230(c)(1) and its progeny dealing with published or shared content. ~~However,~~ Microsoft, however, moves under Section 230(c)(2), not (c)(1).

7. ~~16. Rule 33 of the Consumer Rules of the American Arbitration Association~~
~~provide an arbitrator with authority to dispose of a case at this point in the proceedings.~~ While
often ~~amendment~~amendments of complaints are allowed in the interest of justice, a court can deny
leave to amend when the moving party has shown to ~~this~~the tribunal that amendment

would be futile, which would be the case here. *Bailey v. U.S. Marshals Service Headquarters*, 426 Fed. Appx. 44 (3d Cir. 2011) (“Leave to amend a complaint is futile when the complaint as amended would still be properly dismissed or be immediately subject to summary judgment for the defendant.”) (citations and internal quotations omitted). *See also Wolfington*, 935 F.3d at 195. Claimant is denied an opportunity to amend his complaint for the fifth time, particularly where he submitted his fourth amended claim after having had the benefit of Respondent’s motion for judgment on the pleadings. “Indeed, a ‘district court’s discretion to deny leave to amend is particularly broad where plaintiff has previously amended the complaint.’” *In re Zoom Video Communications Inc. Privacy Litigation*, No.20-CV-02155-LHK, 2021 U.S. Dist. LEXIS 47095, at *23-26 (N.D. Cal. March 11, 2021) (citing *Cafasso, U.S. ex rel Gen. Dynamics C4 Sys., Inc.*, 637 F.3d 1047, 1058 (9th Cir. 2011)).

8. ~~17.~~ Claimant’s breach of contract claims, with the exception of Section F of Count 2 of the Fourth Amended Claim (Windows 10 Breach of EULA), are hereby dismissed. *See Trusted Universal*, 2011 WL 900096, at *8.

9. ~~18.~~ Claimant’s breach of the implied covenant of good faith and fair dealing claims are hereby dismissed. *See Federal Agency of News LLC v. Facebook, Inc.*, 432 F. Supp. 3d 1107, 1120 (N.D. Cal. 2020).

10. ~~19.~~ Claimant’s negligence claims, with the exception of Section E of Count 4 of the Fourth Amended Claim (Windows 10 Negligence), are hereby dismissed. *See Riggs v. Myspace, Inc.*, 2011 WL 3020543, at *1 (9th Cir. July 25, 2011).

11. ~~20.~~ Claimant’s breach of privacy claims are hereby dismissed. *See Poole v. Tumblr, Inc.*, 404 F. Supp. 3d 637, 643 (D. Conn. 2019).

12. ~~21.~~ Claimant’s conversion claims are hereby dismissed. *See Franklin v. X Gear 101, LLC*, 2018 WL 4103492, at *8 (S.D.N.Y. Aug. 28, 2018).

13. ~~22.~~ Claimant’s consumer fraud claims are hereby dismissed. *See e360 Insights*, 546 F. Supp. 2d 605 (N. D. Ill 2008); *In re Zoom Video Communications Inc. Privacy Litigation*, 2021 U.S. Dist. LEXIS 47095, at *65-66.

In light of the Arbitrator’s dismissal of all claims pertaining to Claimant’s OneDrive account, it is hereby ordered that Claimant’s motion to compel Microsoft to produce the image that resulted in his OneDrive account being suspended is DENIED as moot.

Therefore, it is hereby ordered that Respondent’s Motion for the Judgment on a portion of the Pleadings is GRANTED without leave to amend and Claimant’s Motion to Compel is hereby

6

DENIED. The Parties shall submit briefing to address the remaining Windows 10 claims of breach of contract and negligence.

~~Dated: August __, 2021~~

~~THE HONORABLE HARRIET DERMAN, J.S.C.
(Ret), Arbitrator~~

~~By: _____~~

Dated: August 23, 2021

THE HONORABLE HARRIET DERMAN, J.S.C.
(Ret), Arbitrator



By:

Document comparison by Workshare Compare on Monday, August 23, 2021
9:28:55 AM

Input:	
Document 1 ID	file:///C:/Users/nn0/Downloads/Proposed Order Granting Motion for Judgment on the Pleadings.docx
Description	Proposed Order Granting Motion for Judgment on the Pleadings
Document 2 ID	file:///C:/Users/nn0/Downloads/PDF Order Microsoft dismissal.docx
Description	PDF Order Microsoft dismissal
Rendering set	Standard

Legend:	
<u>Insertion</u>	
Deletion	
Moved from	
<u>Moved to</u>	
Style change	
Format change	
Moved deletion	
Inserted cell	
Deleted cell	
Moved cell	
Split/Merged cell	
Padding cell	

Statistics:	
	Count
Insertions	84
Deletions	57
Moved from	12
Moved to	12
Style change	0
Format changed	0
Total changes	165

EXCERPTED EXHIBIT 28

AMERICAN ARBITRATION ASSOCIATION

THOMAS DEUTSCH, ESQ.,	:	
	:	
<i>Claimant,</i>	:	CASE NO. 01-20-0014-3715
	:	
v.	:	
	:	
MICROSOFT CORPORATION,	:	
	:	
<i>Respondent.</i>	:	

**RESPONDENT MICROSOFT CORPORATION'S MOTION TO DISMISS OR FOR
JUDGMENT ON THE PLEADINGS ON CLAIMANT'S WINDOWS 10 BREACH OF
CONTRACT AND NEGLIGENCE CLAIMS**

I. INTRODUCTION

In the Order dated August 23, 2021, the Arbitrator properly dismissed Claimant's claims based on Microsoft's suspension of his OneDrive because Section 230 of the Communications Decency Act protects Microsoft from those claims. That leaves only Claimant's breach of contract and negligence claims arising from the alleged malfunction of Windows 10, which Claimant argues caused him to lose certain files. Despite having amended his demand four times and obtaining discovery, Claimant still has not stated a claim for relief on either ground, and the Arbitrator should dismiss these claims with prejudice.

First, Claimant's breach of contract claim fails because he does not allege essential elements of the claim. In particular, Claimant still (a) has not identified which provision of the end-user licensing agreement ("EULA") he claims Microsoft breached; and (b) has not alleged causation. Indeed, Claimant's own allegations confirm causation is lacking, as he admits that instead of seeking help from Microsoft, he hired non-Microsoft IT technicians who, in the course of performing a reinstallation, caused data to be erased. Because Claimant does not allege facts establishing essential elements of this claim, and in fact pleads allegations undermining them, the Arbitrator should dismiss this claim with prejudice.

Second, the economic loss doctrine bars Claimant's negligence claim because he admits a contract governs his relationship with Microsoft and he bases his negligence claim on the same facts as his contract claim. In any event, Claimant has failed to state a negligence claim because he does not identify a duty independent of the EULA that Microsoft owed to him, much less breach and causation.

II. LEGAL STANDARD

A motion for judgment on the pleadings is evaluated under the same standard as a motion to dismiss for failure to state a claim upon which relief can be granted.¹ *Wolfington v. Reconstructive Orthopedic Assoc. II PC*, 935 F.3d 187, 195 (3d Cir. 2019). Under this standard, "a court must dismiss the plaintiff's complaint if it has failed to articulate a legal basis entitling plaintiff to relief." *Sickles v. Cabot Corp.*, 379 N.J. Super. 100, 105-06 (App. Div. 2005) (citations omitted). In the face of a motion to dismiss or for judgment on the pleadings, plaintiffs "may not rely on conclusory allegations, hoping that discovery will allow them to find that a cause of action exists." *Norcross v.*

¹ Claimant filed the Fourth Amended Claim ("FAC") after Microsoft had answered the Third Amended Claim and had moved to dismiss that demand under Section 230. Given this unique procedural posture, the Arbitrator may consider this as a motion to dismiss or motion for judgment on the pleadings, but either way the standard is the same.

Murphy, 2020 N.J. Super. Unpub. LEXIS 1324, at *18 (N.J. App. Div. July 6, 2020) (citations omitted).

III. ANALYSIS

A. Claimant Has Failed to State a Claim for Breach of Contract, Requiring Dismissal with Prejudice.

Claimant agrees that to state a contract claim, he must allege facts showing “the parties entered into a valid contract, the defendant failed to perform [its] obligations under the contract, and that [he] suffered damages as a result of defendant’s breach.” FAC at 6. Microsoft’s EULA governs the relationship between Microsoft and Windows 10 consumers, such as Claimant. There are two versions of the EULA: one that applies when a customer buys Windows 10 from a device manufacturer or software installer (the “OEM” version); and one for purchases from Microsoft or a retailer (the “retailer” version). See [Retailer EULA](#) (Exhibit 1); [OEM EULA](#) (Exhibit 2); Microsoft’s Answer to Amended Claim ¶ 13, n. 5. Claimant has not alleged how he bought Windows 10, but he admits a contract governs his relationship with Microsoft and under either EULA, his contract claim fails for failure to allege facts establishing breach and causation.²

First, Claimant’s contract claim fails because he does not identify any provision of either EULA that Microsoft allegedly breached. Rather, he refers to Microsoft’s [technical support](#) page, see FAC at 8, n. 6, to argue that Microsoft “guarantees that it will provide Microsoft Windows updates that will terminate if a person’s computer does not have sufficient memory to fully download the update,” *id.* at 8. But Microsoft’s support pages do not create enforceable promises between Microsoft and Claimant. Indeed, both versions of the EULA contain an integration clause that expressly identify what terms comprise the agreements. See [Retailer EULA](#) at ¶ 15 (“This agreement...and the terms contained in web links listed in this agreement, are the entire agreement for the software and any such supplements, updates, and services....”); [OEM EULA](#) at ¶ 14 (“This agreement...and the terms contained in web links listed in this agreement, are the entire agreement for the software and any such supplements, updates, and services....”). The support page upon which Claimant relies is not among the web links referenced in the integration clauses. *P.C. v. Quinn*, 410 N.J. Super. 510, 535 (App. Div. 2009) (for material to be incorporated by reference into an agreement, it “must be described in such terms that its identity may be ascertained beyond doubt”). It therefore is not incorporated into either EULA and is not a term of the agreement between the parties. See, e.g., *Ward v. TheLadders.com, Inc.*, 3 F. Supp. 3d 151, 163 (S.D.N.Y. 2014)

² See, e.g., [Retailer EULA](#); and [OEM EULA](#).

(“[P]laintiffs’ assertion that the representations elsewhere on the website were part of the Terms of Use is deficient and without merit, and therefore, no claim for breach of contract can be based on these representations.”); *In re Facebook Internet Tracking Litig.*, 290 F. Supp. 3d 916, 920 (N.D. Cal. 2017) (finding that data use policy, which included promises not to track logged-out users, was not incorporated by reference into Facebook’s privacy policy), *aff’d in part, rev’d in part and remanded sub nom. In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589 (9th Cir. 2020). As the New Jersey Supreme Court stated in *Harker v. McKissock*, “[t]he essence of voluntary integration is the intentional reduction of the act to a single memorial; and where such is the case the law deems the writing to be the sole and indisputable repository of the intention of the parties.” 12 N.J. 310, 321-22 (1953). In the face of two integration clauses, Claimant cannot state a contract claim based on a non-existent contract provision.

Second, Claimant’s contract claim fails for the independently sufficient reason that his own allegations show he cannot establish causation. Claimant admits that *without* first seeking help from Microsoft, he hired non-Microsoft IT technicians to reinstall Windows 10, and he admits those technicians and that process caused the loss of data. FAC at 3, 9. In Claimant’s own words: “Two career IT professionals ... spent dozens of hours attempting to reinstall Microsoft Windows” and “[r]einstalling Windows had the effect of erasing all of Claimant’s applications, documents, data and backups on his SSD drive.” *Id.* Claimant’s allegations thus confirm his own decisions and actions, and those of the non-Microsoft IT technicians he hired, caused the alleged loss of data—not Microsoft. Claimant therefore has not alleged causation, supplying yet another basis on which the Arbitrator should dismiss the contract claim with prejudice.³

Because Claimant does not, after four amendments, allege a contract term Microsoft supposedly breached or facts showing causation, the Arbitrator should dismiss his Windows 10 claim with prejudice.⁴

³ In his W10 Response submitted on June 25, 2021, Claimant for the first time argued he did not take any action to update his Windows 10 product. *See* Claimant’s June 25, 2021 Response to Motion to Dismiss Windows 10 Claims (“W10 Response”) at 3-4. That plainly contradicts the allegations in his FAC, which state “*Claimant* attempted a customary Microsoft update of his Windows 10 operating system....” FAC at 2. Claimant cannot amend his FAC by opposition to Microsoft’s motion, nor rely on self-serving contradictory statements to circumvent Microsoft’s motion. *See, e.g., Fisher v. Yates*, 270 N.J. Super. 458, 465 (App. Div. 1994) (“litigants must be judicially estopped from asserting a position to the court that ... contradicts their pleadings...”).

⁴ Even if the Arbitrator were to disagree, the Arbitrator should enforce the EULA’s limitation of liability provision, which limits Claimant’s relief to repair, replacement or refund of the Windows 10 software. *See* [Retail EULA](#) at ¶ 9.d.; [OEM EULA](#) at Limited Warranty. New Jersey law recognizes and enforces such limitation of liability provisions, and the Arbitrator should do so here, too, and should at a minimum dismiss with prejudice any claim for damages, injunctive relief, or other relief barred by the limitation of liability provision. *See D’Agostino v. Appliances Buy Phone, Inc.*, 2016 N.J. Super. Unpub. LEXIS 504, at *45 (N.J. Super. Ct. App. Div. Mar. 8, 2016) (applying, as “valid and enforceable,” Google’s limitation of liability provision, which precluded direct, indirect, incidental, special, consequential or exemplary damages, including lost profits, goodwill, use, data or other intangible losses).

B. The Economic Loss Doctrine Bars Claimant's Contract-Based Negligence Claim, Requiring Dismissal with Prejudice.

Claimant's Windows 10 negligence cause of action fails under the economic loss doctrine. That doctrine prohibits a plaintiff "from recovering in tort economic losses to which their entitlement only flows from a contract." *Namerow v. PediatriCare Assoc., LLC*, 461 N.J. Super. 133, 146 (Ch. Div. 2018) (citing *Motors Distrib., Inc. v. Ford Motor Co.*, 98 N.J. 555 (1985) (dismissing plaintiff's tort-based claims as a matter of law where plaintiff alleged that defendant did not fulfill its contractual obligations)). Under "New Jersey law, a tort remedy does not arise from a contractual relationship unless the breaching party owes an independent duty imposed by law." *Saltiel v. GSI Consultants, Inc.* 170 N.J. 297, 316 (2002) (citations omitted) (affirming dismissal of negligent design and negligent misrepresentation in breach of contract case because plaintiff was attempting to use tort allegations to enhance the benefit of the bargain for which she contracted). Therefore, "to bring a tort claim in a case that is primarily a contract claim, the negligence would need to be supported by a separate duty, and that does not exist here." *Dayrit v. Mem'l Hosp. of Slame*, 2012 N.J. Super. Unpub. LEXIS, at *21 (N.J. Super. Ct. App. Div. June 5, 2012); *Saltiel*, 170 N.J. at 317-18 (addressing existence of independent duties imposed by New Jersey law on physicians, attorneys, insurance brokers and manufacturers). Claimant simply "cannot convert basic contract claims into negligence claims." *Saltiel*, 170 N.J. at 318.

Here, Claimant seeks to use a negligence cause of action to obtain a remedy against Microsoft for which he did not bargain. He argues that his negligence claim is "separate and independent from [his] breach of contract claim" because it is based on Microsoft's express policies. *See* W10 Response at 2; FAC at 8-9. But Microsoft has no independent duty to Claimant giving rise to an independent negligence claim under which Claimant may be entitled to relief. And tellingly, Claimant fails to identify any facts establishing such duty. *See, e.g.*, FAC at 8-9. Instead, Claimant's negligence cause of action is explicitly based on "a material breach of the agreement between Claimant and Microsoft on Windows updates."⁵ *See* FAC at 9. *See also* Claimant's W10 Response ("It is undisputed that Microsoft's software and updates, including the Windows 10 update...is governed by the EULA."). As a result, because Claimant's negligence claim is not based on an independent duty and is instead based on the EULA, it is barred by the economic loss doctrine.

⁵ Microsoft has not argued at any point that Claimant's Windows 10 claims are not contract claims. As addressed above, Microsoft instead argues Claimant has failed to identify the applicable EULA which governs the relationship between the parties and that the information and statement on its technical support webpage are not incorporated into the applicable EULA.

Even if the economic loss doctrine did not apply (and it does), as explained above, Claimant has not alleged a breach by Microsoft of any provision of the EULA that could give rise to a negligence claim and does not allege causation. Claimant's admission that non-Microsoft IT technicians caused the data to be erased in attempting to reinstall Windows 10 defeats his negligence claim just as it defeats his contract claim, and the Arbitrator should dismiss this claim with prejudice for this additional reason.

IV. CONCLUSION

For the reasons set forth above, Microsoft respectfully requests that the Arbitrator dismiss the Windows 10 claims with prejudice. Claimant's negligence claim is barred as a matter of law. And Claimant has had multiple opportunities to amend his breach of contract and negligence claims, including three amendments since Microsoft first raised the deficiencies addressed here. His pleadings still suffer the same fatal infirmities, evidencing that any further amendment would be futile and warranting dismissal with prejudice.

Dated: September 10, 2021

RESPONDENT MICROSOFT CORPORATION

By: /s/ Natalie Nahabet
Marc R. Shapiro (NY SBN 4403606)
Natalie Nahabet (CA SBN 301597)
ORRICK, HERRINGTON & SUTCLIFFE LLP
777 South Figueroa Street, Suite 3200
Los Angeles, CA 90017
Telephone: (213) 629-2020
Facsimile: (213) 612-2499
Email: mrshapiro@orrick.com
nnahabet@orrick.com

ATTORNEYS FOR RESPONDENT MICROSOFT
CORPORATION

EXHIBIT 29

AMERICAN ARBITRATION ASSOCIATION

THOMAS DEUTSCH, ESQ.,

Claimant,

CASE NO. 01-20-0014-3715

v.

MICROSOFT CORPORATION,

Respondent.

**CLAIMANT'S OPPOSITION TO
RESPONDENT'S MOTION TO DISMISS OR FOR JUDGMENT ON THE PLEADINGS ON
CLAIMANT'S WINDOWS 10 BREACH OF CONTRACT AND NEGLIGENCE CLAIMS**

INTRODUCTION

Claimant Thomas Deutsch (“Claimant”) brings this consumer arbitration against Respondent Microsoft Corporation (“Microsoft”) on two independent bases: one related to his Microsoft OneDrive account, and a separate and distinct claim related to Microsoft’s faulty Windows 10 update. On August 23, 2021, the Arbitrator dismissed some of the claims alleged in the Fourth Amended Claim related to Claimant’s OneDrive account,¹ but did not dismiss any of Claimant’s Windows 10 claims (collectively, the “Windows 10 Claims”). *See* Order, Aug. 23, 2021. Nor did the Arbitrator rule on Claimant’s claims regarding the enforceability of the limitation on liability and class action waiver found in the Microsoft Service Agreement (“MSA”). *Id.* The Arbitrator then, *sua sponte*,² ordered that Microsoft file a motion to dismiss the Windows 10 Claims.³ Although this arbitration has been pending for over one year, Microsoft has not produced any discovery, documents, or witnesses related to any of the Windows 10 Claims.

ARGUMENT

I. Legal Standard

In a motion to dismiss or for judgment on the pleadings, the Arbitrator must “view the facts presented in the pleadings and the inferences to be drawn therefrom in the light most favorable to the nonmoving party.” *Wolffington v. Reconstructive Orthopaedic Associates*, 935 F.3d 187, 195 (3d Cir. 2019). All of the facts outlined in the claim are to be accepted as true, and the arbitrator may not grant the motion “unless the movant clearly establishes that no material issue of fact remains.” *Id.*; *Zimmerman v. Corbett*, 873 F.3d 414, 417-418 (3d Cir. 2017). A motion to dismiss or for judgment on the pleadings can be granted “only if no relief could be granted under any set of facts that could be proved.” *Syncsort Inc. v. Sequential Software, Inc.*, 50 F. Supp. 2d 318, 324 (D.N.J. 1999). A claim should not be dismissed unless it appears beyond doubt that “the facts alleged in the complaint, even if true, fail to support the claim.” *Id.* at 325. In such review a court or arbitrator has a limited role: “The issue is not whether a plaintiff will ultimately prevail but whether the claimant is entitled to offer evidence to support his [or her] claims.” *Id.*

II. Claimant Has Alleged Facts Sufficient to State a Claim for Breach of Contract

To state a claim for breach of contract, Claimant must allege (1) a contract between the parties; (2) that Microsoft breached the contract; and (3) that Claimant suffered damages as a result of defendant’s

¹ With respect to Claimant’s OneDrive claims—specifically, that Microsoft wrongfully closed Claimant’s OneDrive account, wrongfully precluded Claimant from accessing his files stored on OneDrive, and wrongfully confiscated thousands of Claimant’s files—the Arbitrator dismissed the claims relying exclusively on Section 230 of the Communications Decency Act of 1996 (“CDA”). *See* Order, Aug. 23, 2021. During oral argument, the Arbitrator stated that, even if Microsoft had deemed an image of a soufflé in Claimant’s account to be child pornography and Microsoft failed to take reasonable steps to review the image and correct its error, Section 230 of the CDA still serves as a complete bar to any Claimant recourse. That determination, Claimant asserts, represents a manifest disregard of the law. Claimant also notes that Microsoft drafted the Order—at Microsoft’s request over their concerns of an appeal of the Order—and included in the draft several material misstatements of fact and law that were not discussed or addressed during oral argument.

² Two days prior to the scheduled oral argument on Microsoft’s 230 Motion, and long after the parties submitted their briefs on the motion, the Arbitrator *sua sponte* ordered that Microsoft file a motion to dismiss the Windows 10 Claims. The Arbitrator afforded Microsoft 24 hours to file its motion, and then provided Claimant only half that time to respond. Claimant complied with the Arbitrator’s unduly prejudicial request, noting the impropriety and reserving all rights for appeal.

³ For this motion, the Arbitrator limited Claimant to a response of five pages, double-spaced. The Arbitrator did not provide any legal or factual bases for the limit. This strict limit on a dispositive motion is unduly prejudicial; Claimant reserves all rights for appeal.

breach. *See, e.g., Murphy v Implicito*, 920 A.2d 678, 689 (N.J. App. Div. 2007). Microsoft admits that this legal standard is controlling. *See* Microsoft MJOP on Windows 10 Claims (“MJOP”) at 2. Here, Claimant easily meets the legal threshold.

With respect to the Windows 10 claim for breach of contract, Claimant alleges that Microsoft’s end user license agreement (“EULA”) is the contract at issue with respect to the Windows 10 Claims, and that Microsoft breached the EULA. *See* Fourth Amended Claim at 8. Specifically, with respect to the Windows 10 claim on breach of contract, Claimant explicitly states that “Microsoft Breached the EULA.” *Id.*

Furthermore, Microsoft has admitted that the EULA is the governing contract between the parties with respect to the Windows 10 Claims. *See* MJOP at 2. Contrary to Microsoft’s representations, the law does not require, at this early stage of the matter, that Claimant identify precise provisions in the contract that have been breached. Indeed, Microsoft does not cite to one case—under New Jersey law or otherwise—that mandates that a claimant in a consumer arbitration must identify specific provisions within a contract that have been breached in order to survive a motion to dismiss. In any event, Claimant has provided sufficient details, by indicating that the breach relates to Microsoft providing a faulty Windows 10 update, contrary to its contractual obligations under the EULA. *See* Fourth Amended Claim at 2-3, 8. By providing a faulty update, Microsoft has breached the EULA provisions governing updates (see MJOP, Ex. 1, § 6; MJOP, Ex. 2, § 6) and related warranties (see MJOP, Ex. 1, § 9; MJOP, Ex. 2 at 13-16). Microsoft also breached the EULA provisions governing support procedures for updates (see MJOP, Ex. 1, § 10; MJOP, Ex. 2, § 9).

Finally, Claimant has alleged that he has suffered damages as a result of Microsoft’s breach. Specifically, Claimant states that Microsoft’s mandatory faulty update caused his computer to default to the well-known “Blue Screen of Death,” which blocked Claimant’s access to his entire set of documents and programs. After two experts were unable to resolve the Blue Screen of Death over the course of a month, only a complete reinstallation of the Windows 10 operating system onto Claimant’s computer would allow for its most basic functioning. As a consequence of the necessary reinstallation, all of Claimant’s documents and programs were deleted. Had Claimant done nothing, he would still be frozen out today of any functionality of his computer or Windows 10.⁴ *See* Fourth Amended Claim at 2-3. Claimant specifically alleges that “the Blue Screen of Death causes a computer to freeze without access to Windows, and necessitates a reinstallation of Windows, which erases the hard drive and all files and programs saved to the computer.” *Id.* Still more, Claimant further alleges that Microsoft’s breach of the EULA—by providing a faulty update that caused Claimant’s operating system to generate the Blue Screen of Death—caused him damages: the technical and legal costs incurred to attempt to regain access to his files, and the

⁴ Even if Microsoft had alleged that Claimant had some kind of requirement to contact them beyond what he did in writing, Microsoft does not assert that Microsoft itself could have resolved the Blue Screen of Death. Nor could Microsoft assert that Claimant has a mandate to have only Microsoft address Windows 10 faults. *See* [Nixing the Fix: An FTC Report to Congress on Repair Restrictions](#).

subsequent loss of the documents, data, and programs therein, which are the precise documents and backups that Microsoft OneDrive has in its possession now. *See, e.g., id.*

Indeed, Microsoft does not contest the fact that Claimant has alleged the aforementioned damages—rather, Microsoft attempts to limit its liability by arguing that intervening causes exacerbated the harms to Claimant. MJOP at 3. Yet, this argument goes to the factual extent of Microsoft’s damages, not whether Claimant has alleged facts sufficient to support a breach of contract claim. Microsoft’s failure to cite to any legal authority to support its so-called “independently sufficient reason” for dismissal is a gross misstatement that has zero grounding in New Jersey law.

Taken together, Claimant’s allegations easily meet the threshold requirements to survive a motion to dismiss or for judgment on the pleadings. As mandated by well-established New Jersey precedent, a breach of contract claim cannot be dismissed at this early juncture unless it appears beyond doubt that “the facts alleged in the complaint, even if true, fail to support the claim.” *Syncsort*, 50 F. Supp. 2d at 325. Microsoft has not met—and cannot meet—the high bar for dismissal, and any dismissal at this stage of the Windows 10 breach of contract claim would represent a manifest disregard of New Jersey law.

III. Claimant Has Alleged Facts Sufficient to State a Claim for Negligence

To state a claim for negligence, Claimant must allege the existence of “(1) a duty of care, (2) a breach of that duty, (3) actual and proximate causation, and (4) damages.” *Jersey Cent. Power & Light Co. v. Melcar Util. Co.*, 212 N.J. 576, 594 (2013). Claimant easily meets this legal threshold. As he details:

Among its obligations and duties, Microsoft has a duty to act in a reasonable manner and follow its own policies. One such policy is that Microsoft states it will create Windows 10 updates that auto-stop and create an alert if a user’s computer does not have sufficient memory to install the update. Microsoft breached its duty with respect to Claimant because Microsoft provided Claimant with a Microsoft Windows 10 update that did not maintain a safeguard that pauses the update in the event a user’s hard drive does not have sufficient memory to install the update. When Claimant was installing the update provided by Microsoft, his SSD drive did not have sufficient memory to install the update. But, the update did not stop. Rather, it crashed Claimant’s computer, which necessitated a Windows reinstallation, causing Claimant to lose all the programs, documents, data and backups saved on his SSD drive. Microsoft’s acts and omissions are both an actual and proximate cause of harm to Claimant, which includes but is not limited to Claimant’s inability to access and utilize his documents. Claimant has suffered extensive damages because of the breach, which include but are not limited to, economic and other harm due to the inability to access his documents, and costs and attorneys fees to bring this action. Fourth Amended Claim at 12-13.

In short, Claimant alleges that Microsoft had a duty to engage in reasonable conduct in mandating and providing Windows 10 updates, that Microsoft breached that duty because the company provided Claimant with a faulty Windows 10 update that caused his operating system to prevent access to all of his programs and documents, and that Microsoft’s breach is both a cause-in-fact and proximate cause of damages to Claimant. *Id.* With respect to damages, Claimant alleges the financial harms caused by the aforementioned, and furthermore alleges harms to his personal and professional life. *Id.* at 21.

Microsoft merely offers conclusory statements—without citing any legal authority—in arguing that Claimant’s allegations are insufficient. MJOP at 5. Rather, all that Microsoft contests is the extent of

damages, pointing to intervening causes that might limit Microsoft's liability. At this stage of the matter, however, the extent of Microsoft's damages is irrelevant to whether Claimant has alleged facts sufficient to state a claim. For the foregoing reasons, the Windows 10 negligence claim allegations are sufficient to survive a motion to dismiss or for judgment on the pleadings, and this claim should move to discovery.

IV. The Economic Loss Doctrine Does Not Support Dismissal of the Negligence Claim

Microsoft contends that, under the economic loss doctrine, a tort remedy cannot arise from a contractual relationship unless the breaching party owes an independent legal duty. MJOP at 4. However, as the New Jersey Supreme Court has established, an independent duty can be created when the contracting party makes representations regarding itself or the product that are above and beyond those contained in the contract. *Saltiel v. GSI Consultants, Inc.*, 788 A.2d 268, 279 (N.J. 2002). Further, as *Saltiel* paraphrases *Flintkote Co. v. Dravo Corp.*, 678 F.2d 942, 946 (11th Cir. 1982), "recognizing that duties can be imposed on manufacturers and suppliers independent of contract, such as duty to use reasonable care not to place defective products in the market." Here, Microsoft made representations on their own website—and not contained in the EULA—regarding the Windows 10 software update auto-stopping and alerting a Windows 10 user when the user's computer did not have sufficient memory to install the update.⁵ By making these representations, Microsoft created and owed Windows 10 users, such as Claimant, a duty consistent with that representation; a duty which they breached, and which ultimately caused Claimant's damages when his computer generated the Blue Screen of Death, blocking Claimant's access to his documents, data and programs, and causing Claimant to lose all of his documents, data and programs on his computer upon the necessary Windows 10 reinstallation.

Further, while the economic loss doctrine generally prevents a plaintiff's recovery "in tort [of] economic losses to which their entitlement flows only from a contract," MJOP at 4, a clear and specific exception has been recognized by New Jersey and the Third Circuit which allows a plaintiff to recover in tort when the plaintiff suffers damage to other property which was not the subject of, nor the benefit to be received by the plaintiff from, the contract at issue. *See, e.g., 2J Corp. v. Tice*, 126 F.3d 539, 542-545 (3d Cir. 1997) (finding that the plaintiff could maintain a negligence action and recover damages for the *contents* of a collapsed warehouse, where the construction of the warehouse itself was the subject of the contract); *Alloway v. Gen. Marine Indus., L.P.*, 149 N.J. 620, 627 (N.J. 1997) ("[T]ort principles are better suited to resolve claims for ... damages to other property."). This same concept is clear in Microsoft's citation to *Saltiel v. GSI Consultants, Inc.*, *supra*, for the proposition that a plaintiff cannot "use tort allegations to enhance *the benefit of the bargain for which she contracted*." MJOP at 4 (emphasis added). In *Saltiel*, no damage was incurred by Plaintiff, that gave rise to negligence claims, separate and apart from the deficient contractual work that the Defendant performed. Here, Claimant and Microsoft entered into

⁵ <https://support.microsoft.com/en-us/windows/free-up-space-for-windows-updates-429b12ba-f514-be0b-4924-ca6d16fa1d65>.

two separate and distinct contracts—the MSA governing their relationship as to the storage and safekeeping of Claimant’s private files on OneDrive, and the EULA, governing their relationship as to Microsoft’s Windows 10 software. The sole property subject to, and bargained for, by Claimant as it related to the EULA was the Microsoft Windows 10 software.

Microsoft’s Windows 10 software is the sole property subject to the EULA. But similar to the contents of the warehouse in *2J Corp.*, Claimant’s documents, files, and data constitute “other property.” Thus, Claimant cannot be prohibited, under the economic loss doctrine, from recovery based on Microsoft’s negligence—which resulted in the non-contractual loss of Claimant’s documents, data, and programs—and which was caused by a failure of Microsoft’s software to perform in accordance with Microsoft’s expressed, detailed policies and non-contractual representations.

V. Insofar as the Motion Is Granted Due to a Pleading Deficiency, Claimant Respectfully Requests Leave to Amend the Pleadings

Insofar as the motion is granted due to a pleading deficiency that may be cured, Claimant respectfully requests leave to amend the pleadings. As courts in New Jersey have consistently and routinely held, “leave to amend a pleading shall be freely given in the interest of justice.” *Hansen v. Hansen*, 770 A.2d 1278, 1286 (N.J. App. Div. 2001). “[M]otions for leave to amend should be treated indulgently and leave should be freely given in the interest of justice.” *Id.*

This matter has had no discovery related to the Windows 10 Claims, and thus Claimant has not been afforded an opportunity to investigate and address Microsoft’s wrongful and negligent conduct. To date, the arbitration has focused exclusively on Claimant’s OneDrive claims, and Claimant’s previous amendments came after the limited discovery in this matter produced new, material evidence regarding Microsoft’s wrongdoing regarding OneDrive. Since there has been no discovery, nor any amendments to the Claim related to the Windows 10 Claims, granting the pending motion at this stage of the arbitration would represent a manifest disregard for Claimant’s legal rights. Given the procedural posture of the Windows 10 Claims, to the extent the motion is granted due to a pleading deficiency that may be cured, Claimant respectfully requests that the Arbitrator grant leave to amend.

CONCLUSION

For the reasons outlined herein, Claimant respectfully requests that the Arbitrator deny Microsoft’s motion and allow this matter to proceed to discovery.

Dated: October 4, 2021

SALZANO, LAMPERT & WILSON, LLP

By: /s/ Frank Salzano

Frank Salzano, Esq. (NY SBN 4114849)
275 Madison Avenue, 35th Floor
New York, New York 10016
(646) 863-1883
fsalzano@slwlawoffices.com
Attorneys for Claimant

EXCERPTED EXHIBIT 30

AMERICAN ARBITRATION ASSOCIATION

THOMAS DEUTSCH, ESQ.,	:	
	:	
<i>Claimant,</i>	:	CASE NO. 01-20-0014-3715
	:	
v.	:	
	:	
MICROSOFT CORPORATION,	:	
	:	
<i>Respondent.</i>	:	

**RESPONDENT MICROSOFT CORPORATION’S REPLY IN SUPPORT OF MOTION
TO DISMISS OR FOR JUDGMENT ON THE PLEADINGS ON CLAIMANT’S
WINDOWS 10 BREACH OF CONTRACT AND NEGLIGENCE CLAIMS**

I. INTRODUCTION

In his Fourth Amended Claim (“FAC”), Claimant alleged Microsoft breached the EULA by failing to adhere to “terms” outside it, namely, representations on Microsoft’s customer support page. Claimant now abandons that theory. However, a party cannot amend a complaint through an opposition, as Claimant does here. In any event, his new theories are unavailing. The only provision even remotely applicable here—the software warranty—expired two years before the complained-of incident. Furthermore, because any damages arose from reinstallation of the software and reinstallation was performed by non-Microsoft technicians, Claimant cannot demonstrate causation. That resolves Claimant’s breach of contract claim and, in turn, the litigation as a whole. That is because the parties’ Windows 10 relationship is governed entirely by the EULA. Indeed, the EULA addresses the subject matter of this dispute (Windows 10 updates), the challenged conduct (software performance), the duration of any obligation (warranties), and all damages (to software and otherwise). Accordingly, Claimant’s Windows 10 breach of contract and negligence claims should be dismissed.

After four amendments, it is now evident that any further amendment would be futile. Claimant’s opposition, which presages the contents of a fifth amendment, evinces as much. It injects new theories that are no more availing than the original ones and introduces contradictory assertions all in service of avoiding the economic loss rule. What is now clear is that Claimant will continue to manufacture new theories, but after multiple amendments he still cannot articulate a cognizable cause of action in the face of the EULA. The arbitrator should dismiss Claimant’s Windows 10 claims with prejudice.

II. ARGUMENT

a. Claimant Fails to State a Claim for Breach of the EULA

As Microsoft explained (Mot. 2-3), Claimants’ breach of contract claim fails because he identifies no term of the EULA that Microsoft breached. Instead, Claimant’s cause of action looks outside the contract, pointing to Microsoft’s support page. FAC 8. Mr. Deutsch asserts that is permissible because “the law does not require, at this early stage of the matter, that Claimant identify precise provisions in the contract that have been breached.” Opp. 2. Claimant is wrong. “Under New Jersey law, a complaint alleging breach of contract must, at a minimum, identify the contracts and provisions breached.” *Eprotec Pres., Inc. v. Engineered Materials, Inc.*, 2011 U.S. Dist. LEXIS 24231, at *22 (D.N.J. Mar. 9, 2011). “Failure to allege the specific provisions of contracts breached is grounds for dismissal.” *Id.* at *23; *SAT Agiyar, LLC v. 7-Eleven, Inc.*, 2020 U.S. Dist. LEXIS 116762, at *9 (D.N.J. June 30, 2020) (same); *MacFarlane v. Southern Jersey Family Medical*

Centers, Inc., 2021 N.J. Super. Unpub. LEXIS 1950, at *52 (N.J. Super. Ct. App. Div. Aug. 30, 2021) (affirming trial court’s dismissal for failure to identify provision of agreement allegedly breached). Though Claimant insists he has met this threshold obligation, all he offers are generic references to pages “2-3, 8” of his complaint. Opp. 2. Nowhere on those pages does the FAC identify any specific provision of the EULA.

Now, *for the first time*, in his opposition, Claimant cites particular provisions he claims Microsoft breached. Opp. 2 (citing EULA’s provisions concerning warranties, support procedures, and updates). However, a “complaint may not be amended by the briefs in opposition to a motion to dismiss.” *Penn. ex rel. v. Zimmerman v. Pepsico*, 836 F.2d 173 (3d Cir. 1988). Regardless, these new, citation-only allegations are unavailing. First, there can be no breach of the EULA’s warranty provision because the warranty (at its latest) lasted one year from the date of purchase. Mot., Ex. 1 ¶ 9; Ex. 2 at 13. Here, Claimant acquired the software in August 2017 and he challenges conduct that occurred in June 2020. *See* Exhibit 1, Claimant’s Response to Respondent’s First Set of Interrogatories No. 2 (device on which Windows 10 software came pre-installed was purchased “not long after August 16, 2017”);¹ FAC 2 (complaint discussing incident in June 2020). Second, Claimant cannot demonstrate a breach of the EULA’s support provision (Mot., Ex. 1 ¶ 10; Ex. 2 ¶ 9) because he did not acquire support from *Microsoft*. His own allegations state he utilized the services of third-party technicians. FAC 3. Third, Microsoft cannot have violated the EULA’s update provision because Microsoft has no obligations under that clause. The update provision notifies users that “[t]he software periodically checks for system and app updates, and downloads and installs them.” Mot., Ex. 1 ¶ 6; Ex. 2 ¶ 6. The only obligation included is *on the part of the user* who “agree[s] to receives these types of automatic updates without any additional notice.” *Id.*

Claimant’s newly-contrived causation arguments are also unavailing. Claimant now asserts any damage occurred when he was unable to access his data. Opp. 2. However, the inability to access files is different than destroying them. Claimant’s cause of action is predicated upon the latter. He alleges the act of “[r]einstalling Windows, had the effect of erasing all of Claimant’s applications, documents, data and backups on his SSD drive.” FAC 9. He further alleges the reinstallation was conducted by “[t]wo career IT professionals.” *Id.* at 3. Having declined to utilize Microsoft services, Claimant cannot claim Microsoft caused any injury arising out of reinstallation.

¹ This Court may consider discovery responses in determining futility of amendment. *See, e.g., Canales v. Yue Yu*, 2020 N.J. Super. Unpub. LEXIS 456, at *12 (N.J. Super. Ct. App. Div. Mar. 4, 2020) (judge must consider “whether granting amendment would nonetheless be futile”; while “leave to amend should be decided ‘without consideration of the ultimate merits of the amendment,’ the judge must consider ‘the factual situation existing at the time [the] motion is made’”).

Finally, Microsoft does not dispute that Claimant has alleged damages. But, as it has explained, those damages are limited by the EULA, precluding any recovery beyond “repair, replacement, or refund” of the Windows 10 software.² Mot. 3 n. 4. What’s more, Claimant now disavows any recovery beyond damages to the software itself. *See* Opp. 5 (“The sole property subject to, and bargained for, by Claimant as it related to the EULA was the Microsoft Windows 10 software.”). Nonetheless, as explained further below, Microsoft disagrees with Claimant’s characterization of the scope of the parties’ contract.

b. Claimant Fails to State a Claim for Negligence Relating to Windows 10

Claimant’s negligence claim alleges Microsoft breached its duty to him by failing to “create Windows 10 updates that auto-stop and create an alert if a user’s computer does not have sufficient memory to install the update.” FAC 12. That alleged failure mirrors the allegations underlying Claimant’s breach of contract claim. FAC 9 (alleging Microsoft breached by “guarantee[ing] that [it] will provide Microsoft Windows updates that will terminate if a person’s computer does not have sufficient memory” by “check[ing] to make sure there’s enough storage space on [the] device”). Because a party cannot “recover[] in tort” for “economic losses to which their entitlement flows from a contract,” Claimant’s negligence claim is barred by the economic loss rule. *Namerow v. PediatriCare Assoc., LLC*, 461 N.J. Super. 133, 146 (Ch. Div. 2018). In response to Microsoft’s motion, Claimant now argues only his negligence claim (not his breach of contract claim) relies on the company’s support pages; this distinction, he contends, supplies the requisite independent duty to avoid dismissal under the economic loss doctrine. Opp. 4. Claimant is wrong.

Whether a tort claim is viable in the face of a contract between two parties “depends on whether the tortious conduct alleged is extrinsic to the contract between the parties.” *Chen v. HD Dimension, Corp.*, 2010 U.S. Dist. LEXIS 120599, at *26 (D.N.J. Nov. 15, 2010). Here, the subject matter of the tortious conduct alleged—updates and software functionality—is *not* extrinsic to the contract. The EULA states, “[t]his agreement applies to the Windows software that is preinstalled on your device ... and also any Microsoft *updates*, upgrades, supplements or services for the software, unless other terms come with them.” Mot., Ex. 1 ¶ 1.a; Ex. 2 ¶ 1.a (emphasis added). It also expressly addresses how the software will perform, stating, “Microsoft...warrants that properly licensed software will perform substantially as described in any Microsoft materials³ that accompany the software.” *Id.* at Ex. 1 ¶ 9.a; Ex. 2 at 13. Furthermore, the EULA expressly states,

² This necessarily precludes any effort by Claimant to use his Windows 10 claims to acquire the same relief (data recovery) that he was denied through the Arbitrator’s Section 230 ruling.

³ Claimant does not allege, nor can he, that the technical support webpage was included in the “materials that accompany the software.”

“Microsoft... [does not] give[] any other express warranties, guarantees, or conditions” and “exclude[s] all implied warranties and conditions, including those of merchantability, fitness for a particular purpose, and non-infringement.” Mot., Ex. 1 ¶ 9.b; Ex. 2 at 13. Accordingly, any statements on Microsoft’s website concerning updates and software functionality are irrelevant because the parties agreed such issues would be resolved exclusively pursuant to the EULA. *See, e.g., Montclair State Univ. v. Oracle USA, Inc.*, 2012 U.S. Dist. LEXIS 119509, at *15 (D.N.J. Aug. 23, 2012) (“[A]n alleged misrepresentation that ‘involve[s] a nonfulfillment of a warranty or guarantee contained within the contract itself’ cannot be said to be extraneous to the contract.”) (citation omitted); *Blanos v. Penn Mut. Life Ins. Co.*, 2010 U.S. Dist. LEXIS 2326, at *15-16 (D.N.J. Jan. 12, 2010) (integration clause and disclaimer provisions of agreement barred any claims based on representations not included in the terms of the contract).

Claimant attempts a similar gambit by attempting to differentiate between types of damage. Specifically, Claimant argues a plaintiff can “recover in tort when the plaintiff suffers damage to other property which was not the subject of, nor the benefit to be received by the plaintiff from, the contract at issue.” Opp. 4. From there, he asserts the “sole property subject to, and bargained for, by Claimant as it related to the EULA was the Microsoft Windows 10 software.” *Id.* “[D]ocuments, files, and data constitute,” he argues, “‘other property.’” *Id.* That contention is at odds with Claimant’s causation-related breach of contract argument (wherein he asserts damages occurred when “documents and programs were deleted,” Opp. 2) and, in any event, the distinction is artificial under both the case law and the EULA. Under New Jersey law, “[w]hen...a product fails to fulfill a purchaser’s economic expectations, contract principles...provide a more appropriate analytical framework.” *Travelers Indem. Co. v. Dammann & Co., Inc.*, 592 F. Supp. 2d 752, 760-61 (D.N.J. 2008). To determine the parties’ expectations, courts look to whether “damage that occur[red] is at the core of the [parties’] commercial transaction” and was “contemplated by the parties” in the agreement. *Id.*

In re Merritt Logan, 901 F.2d 349 (3d Cir. 1990), is instructive. There, the buyer of a defective refrigeration system sued the manufacturer, installer and seller of the system, asserting tort theories for damage to the food that spoiled when the refrigeration system failed. The Third Circuit held, under New Jersey law, there was no viable tort claim because the damage to plaintiff’s food was at the core of the transaction. *Id.* at 362; *see also International Flavors & Fragrances, Inc. v. McCormick & Co., Inc.*, 575 F. Supp. 2d 654 (D.N.J.2008) (damage to barbeque seasoning into which defective paprika was incorporated did not constitute a viable tort claim under the economic loss doctrine). Here, the damage alleged is at the “core of the transaction.” The transaction was the

sale of Windows 10. All the damages asserted (lost data and electronic files) are of the sort that would naturally be contemplated by the sale of software. *See Saltiel v. GSI Consultants, Inc.*, 170 N.J. 297, 316 (2002) (“When a company agrees to render a service or sell a product, a contract normally will define the scope of the parties’ specific obligations.”).⁴ Indeed, the EULA’s damages provision makes that clear. It is not limited to “repair, replacement, or refund” of the software but rather contemplates and addresses other, non-software related damages, including for “lost profits, or direct, consequential, special, indirect, or incidental damages.” Mot., Ex. 1 ¶ 9.d; Ex. 2 at 13. Claimant’s split-property-damages theory therefore does not save him from application of the economic loss rule.

Even if the economic loss rule did not apply, Claimant’s negligence claim fails on the same causation grounds as his breach of contract claim. *See supra* II.a.

c. Amendment Would Be Futile and the FAC Should be Dismissed with Prejudice

After four amendments, a recent opposition that amounts to a fifth, and (contrary to Claimant’s contention) discovery on the Windows 10 issue,⁵ Claimant has still not alleged any term of the EULA that Microsoft breached or identified an independent basis that would allow a negligence claim to proceed in the face of the EULA. “[T]here is no point to permitting the filing of an amended pleading when a subsequent motion to dismiss must be granted.” *Mustilli v. Mustilli*, 287 N.J. Super. 605, 607 (Ch. Div. 1995). Claimant’s opposition reveals that any allegations in a fifth amended complaint would suffer the same infirmities.

III. CONCLUSION

For the reasons discussed in the Motion and above, Microsoft respectfully requests that the Arbitrator dismiss the Windows 10 claims with prejudice.

[Signature on Following Page]

⁴ Claimant’s reliance on *2J Corp. v. Tice*, 126 F.3d 539 (3d Cir. 1997) is misplaced where it involves the application of Pennsylvania law and did not involve a contract like the EULA which defined the scope of the parties’ obligations and potential damages.

⁵ Contrary to Claimant’s contention, the parties have engaged in, and exchanged, discovery concerning the Windows 10 issue and Microsoft has responded to them. *See, e.g.*, Ex. 1, Claimant’s Responses to Microsoft’s Interrogatory Nos. 2-3, 7; Ex. 2, Claimant’s Request for Production of Documents (“RFP”) No. 7, 9; Ex. 3, Microsoft’s RFP Nos. 1-3; and Ex. 4, Claimant’s Interrogatory Nos. 5-6.

Dated: October 15, 2021

RESPONDENT MICROSOFT CORPORATION

By: /s/ Natalie Nahabet
Marc R. Shapiro (NY SBN 4403606)
Natalie Nahabet (CA SBN 301597)
ORRICK, HERRINGTON & SUTCLIFFE LLP
777 South Figueroa Street, Suite 3200
Los Angeles, CA 90017
Telephone: (213) 629-2020
Facsimile: (213) 612-2499
Email: mrshapiro@orrick.com
nnahabet@orrick.com

EXCERPTED EXHIBIT 31

AMERICAN ARBITRATION ASSOCIATION

THOMAS DEUTSCH, ESQ.,

Claimant,

CASE NO. 01-20-0014-3715

v.

MICROSOFT CORPORATION,

Respondent.

(Telephone conference)

December 1, 2021

4:03 p.m. EST

MOTION TO DISMISS OR FOR
JUDGMENT ON THE PLEADINGS
ON CLAIMANT'S WINDOW 10 BREACH
OF CONTRACT AND NEGLIGENCE CLAIMS

BEFORE:

HONORABLE HARRIET DERMAN

<p style="text-align: right;">Page 2</p> <p>1 APPEARANCES:</p> <p>2 ORRICK, HERRINGTON & SUTCLIFFE LLP</p> <p>3 ATTORNEYS FOR RESPONDENT MICROSOFT CORPORATION</p> <p>4 777 South Figueroa Street, Suite 3200</p> <p>5 Los Angeles, CA 90017</p> <p>6 BY: Marc R. Shapiro, Esq.</p> <p>7 Natalie Nahabet, Esq.</p> <p>8</p> <p>9 SALZANO, LAMPERT, AND WILSON LLP</p> <p>10 ATTORNEYS FOR CLAIMANT</p> <p>11 275 Madison Avenue, 35th Floor</p> <p>12 New York, NY 10016</p> <p>13 BY: Efthimos Parasidis, Esq.</p> <p>14</p> <p>15 ALSO PRESENT:</p> <p>16 Thomas Deutsch, Esq. - Claimant</p> <p>17</p> <p>18 DiFrancesco, Bateman, Coley, Yospin, Kunzman, Davis,</p> <p>19 Lehrer & Flaum, P.C.</p> <p>20 15 Mountain Boulevard</p> <p>21 Warren, NJ 07058</p> <p>22 BY: HONORABLE HARRIET DERMAN</p> <p>23 Michael Solvert - Associate</p> <p>24</p> <p>25</p>	<p style="text-align: right;">Page 4</p> <p>1 Although they relied on a new argument</p> <p>2 that the support page provided independent</p> <p>3 duty, that's simply not the case here because</p> <p>4 the software updates and software functionality</p> <p>5 are just not extended to the contract between</p> <p>6 the parties, so we can't assert a tort claim.</p> <p>7 The law specifically states that it applies to</p> <p>8 Windows updates and how the software will</p> <p>9 perform. It doesn't claim any other expressed</p> <p>10 warranties, guarantees, or conditions, as well</p> <p>11 as implied warranties and conditions. And as</p> <p>12 the Montclair State University and the Blanos</p> <p>13 cases demonstrate, his negligence claim simply</p> <p>14 can't be extraneous to the contract.</p> <p>15 Finally, his attempt to argue that his</p> <p>16 data is, quote/unquote, other property which</p> <p>17 was damage is unrevealing because a court looks</p> <p>18 at whether the damage that occurred is at the</p> <p>19 core of the parties' transaction and</p> <p>20 contemplated by the parties. Similar to the</p> <p>21 Merritt Logan case where the court found that</p> <p>22 there was no viable tort claim for damage to</p> <p>23 plaintiff's food based on a defective</p> <p>24 refrigeration system. Here, the damages</p> <p>25 asserted are also contemplated by the sale of</p>
<p style="text-align: right;">Page 3</p> <p>1 (Time noted: 4:03 p.m.)</p> <p>2 JUDGE DERMAN: Let's begin then.</p> <p>3 This is Microsoft's motion to dismiss or</p> <p>4 for judgments on the pleadings.</p> <p>5 We have two counts left. I've read</p> <p>6 everything.</p> <p>7 And so, Ms. Nahabet, you can give me your</p> <p>8 best points.</p> <p>9 MS. NAHABET: Thank you, Your Honor.</p> <p>10 I'll just start with the fact that the</p> <p>11 parties don't dispute that there's a contract</p> <p>12 that's governed here. I'll get into the</p> <p>13 contract in a moment, but the fact that there</p> <p>14 is one precludes any negligence claim. The</p> <p>15 economic loss doctrine prohibits claimant from</p> <p>16 recovering in tort economic lawsuit to which</p> <p>17 the entity is entitled to only those from the</p> <p>18 contract and licensing agreement.</p> <p>19 Claimant has not established an</p> <p>20 independent duty imposed by law through which</p> <p>21 we can allege a tort. His fourth amended</p> <p>22 complaint is explicitly based on a material</p> <p>23 breach of the agreement between claimant and</p> <p>24 Microsoft on Windows updates and that's in the</p> <p>25 fourth amendment complaint at page 9.</p>	<p style="text-align: right;">Page 5</p> <p>1 software, particularly for the EULA's damages</p> <p>2 provision isn't limited just to software</p> <p>3 related damages, it covers other damages as</p> <p>4 well.</p> <p>5 Moving to the breach of contract claim.</p> <p>6 Claimant's fourth amended claim does not</p> <p>7 identify any provision of the EULA, the</p> <p>8 End-User Licensing Agreement, which he claimed</p> <p>9 Microsoft breached. That alone means that the</p> <p>10 complaint must be dismissed. New Jersey law</p> <p>11 states a complaint must, at minimum, identify</p> <p>12 the contracts and the provisions breached or</p> <p>13 otherwise be dismissed as stated in the Eprotec</p> <p>14 Preservation case.</p> <p>15 While he attempts to identify some</p> <p>16 provisions in his opposition, it's clear that</p> <p>17 allowing him to amend alleged breach of those</p> <p>18 new provisions would be skewed file and there</p> <p>19 are three of them. The provisions include</p> <p>20 warranties, support procedures, and updates.</p> <p>21 The first is the warranty, that has long</p> <p>22 since expired since claimant acquired the</p> <p>23 software in August 2017 and the alleged conduct</p> <p>24 that he complains of here occurred in June of</p> <p>25 2020.</p>

<p style="text-align: right;">Page 6</p> <p>1 Second, he didn't acquire any support from</p> <p>2 Microsoft, instead, he was using his own</p> <p>3 third-party technician, so we can't allege a</p> <p>4 breach of that provision either.</p> <p>5 Third, with regard to the update</p> <p>6 provision, Microsoft has no obligations under</p> <p>7 that cause since it notifies its users that the</p> <p>8 software will be periodically updated.</p> <p>9 Moving on to causation. Claimant has not</p> <p>10 established that Microsoft caused the loss of</p> <p>11 his data where he admits that a</p> <p>12 non-Microsoft -- or wasn't one -- non-Microsoft</p> <p>13 IT technician reinstalled the Windows 10 and</p> <p>14 that reinstalling Windows 10 had the effect of</p> <p>15 erasing his data.</p> <p>16 Again, in his opposition, he asserts a new</p> <p>17 series of damages occurred when he was unable</p> <p>18 to access his data but that's different than</p> <p>19 destroying them and his demand is actually</p> <p>20 focused on the latter, the destruction of the</p> <p>21 data.</p> <p>22 Finally --</p> <p>23 JUDGE DERMAN: Could you elaborate on that</p> <p>24 last point, please?</p> <p>25 MS. NAHABET: So, do you mean with regard</p>	<p style="text-align: right;">Page 8</p> <p>1 I'm happy to address them before I move on.</p> <p>2 JUDGE DERMAN: It's one thing to focus on</p> <p>3 damage, but it's another thing to say that he</p> <p>4 can't access it.</p> <p>5 MS. NAHABET: Yes, the destruction versus</p> <p>6 the access, exactly.</p> <p>7 JUDGE DERMAN: We know that he's already</p> <p>8 limited by Section 230 as to access, but</p> <p>9 presumably if he had a viable claim, let's say</p> <p>10 he did raise destruction, which is different</p> <p>11 than inability to access, could be something</p> <p>12 that for which he's seeking relief.</p> <p>13 MS. NAHABET: So, in his fourth amendment</p> <p>14 complaint, he is seeking relief for the</p> <p>15 destruction. In opposition, he's trying to</p> <p>16 find a new argument in respect to the loss of</p> <p>17 the access loss that he's also entitled to</p> <p>18 relief from is the point that I'm trying to</p> <p>19 make.</p> <p>20 JUDGE DERMAN: Thank you.</p> <p>21 MR. SHAPIRO: Judge, I apologize. It's</p> <p>22 Mark. I would just chime that I think if we're</p> <p>23 talking about damages due to inability to</p> <p>24 access, that's obviously not the factual state</p> <p>25 of things at this moment, so we would just be</p>
<p style="text-align: right;">Page 7</p> <p>1 causation about the non-IT technicians?</p> <p>2 JUDGE DERMAN: Right after that I think</p> <p>3 you mentioned something about damages.</p> <p>4 He was unable to access. So,</p> <p>5 approximately, at that time, I couldn't follow</p> <p>6 you.</p> <p>7 MS. NAHABET: He's claiming in his</p> <p>8 opposition he's asserting that the damage</p> <p>9 occurred when he was unable to access his data</p> <p>10 but that's different than the destruction of</p> <p>11 the data, which is what his complaint is based</p> <p>12 off of. In his complaint, he said that</p> <p>13 reinstalling Windows had the effect of erasing</p> <p>14 all of his applications, documents, data, and</p> <p>15 the back up on his SSD drive, so that's really</p> <p>16 what the focus is. But then in his opposition,</p> <p>17 this new argument he tries to make is that he</p> <p>18 was unable to access his data which he already</p> <p>19 addresses with the Section 230 motion and with</p> <p>20 regard to his One Drive. He's precluded from</p> <p>21 trying to use his Windows 10 claim to acquire</p> <p>22 the same relief which is the data recovery that</p> <p>23 he was denied through Your Honor's Section 230</p> <p>24 ruling.</p> <p>25 If you have any further questions on them,</p>	<p style="text-align: right;">Page 9</p> <p>1 talking about damages during the time period</p> <p>2 for which he was unable to access and then</p> <p>3 there was a subsequent destruction, which is</p> <p>4 obviously not what we're dealing with on the</p> <p>5 facts of the case anymore.</p> <p>6 JUDGE DERMAN: Well, okay, I'll come back</p> <p>7 to that later. That's relevant to a question I</p> <p>8 have.</p> <p>9 Go ahead.</p> <p>10 MS. NAHABET: Thank you, Your Honor.</p> <p>11 Finally, claimant disavowed any recovery</p> <p>12 beyond damages to the software itself by</p> <p>13 stating, "The sole property subject to, and</p> <p>14 bargained for, by Claimant as it related to the</p> <p>15 EULA was the Microsoft Windows 10 software."</p> <p>16 We addressed that in the briefing, but he</p> <p>17 disavows any recovery beyond damages to the</p> <p>18 software. We just wanted to point that out.</p> <p>19 Finally, with regard to the amendment,</p> <p>20 he's amendment it about 4 times already, even</p> <p>21 after being on notice of the decisions based</p> <p>22 off of the numerous answers that Microsoft has</p> <p>23 submitted. His opposition effectively operates</p> <p>24 as new arguments as to what we could expect to</p> <p>25 see in a fifth amended complaint and based off</p>

<p style="text-align: right;">Page 10</p> <p>1 of data that we've addressed in the briefing, 2 it's clear that he would still fail to make the 3 requisite showing. 4 Thank you, Your Honor. 5 JUDGE DERMAN: Mr. Parisidis? 6 MR. PARASIDIS: Thank you, Your Honor. 7 There are three general points I'd like to 8 make; first, some general principles about this 9 motion; second, I'll speak to claimant's 10 contract claims; and third, I'll speak to his 11 negligence claims. 12 To begin with, the general principles, 13 it's important to remember that at this stage 14 of this arbitration, a motion to dismiss or for 15 judgment on the pleadings should only be 16 granted if no relief could be granted under any 17 set of facts that could be proved. The issue 18 is not whether claimant will ultimately prevail 19 but whether claimant is entitled to offer 20 evidence to support his claim. So, we're at a 21 very early stage in this case. 22 Another preliminary point to raise is that 23 Microsoft did not request to file this motion 24 to dismiss. That request was made by Your 25 Honor via sua sponte request. I think it's</p>	<p style="text-align: right;">Page 12</p> <p>1 Now, to get into the details of the breach 2 contract claim, it's clear that the EULA 3 applies here but it's not the sole document 4 that is relevant to this breach of contract 5 claim. Also relevant are Microsoft's 6 representation that they will provide updates 7 that are not faulty and that also has been 8 referenced in the amended complaints and as 9 well in the briefs. 10 Now, here, in particular, when claimant 11 purchased this Microsoft software, it came 12 bundled with his Dell computer, the laptop 13 computer, and in those instances Microsoft 14 requires, via this license agreement with Dell 15 that then gets passed down to claimant, that 16 claimant needs to first reach out to Dell, 17 which he did, and then Dell told him to reach 18 out to Microsoft, which he also did, and 19 Microsoft never responded. It was after 20 Microsoft failed to respond, Dell computer said 21 it had no ability to respond because the 22 failure was due to do Microsoft's faulty 23 Windows update. And at that point, claimant 24 paid out of his own pocket to have IT 25 professionals try to figure out what was going</p>
<p style="text-align: right;">Page 11</p> <p>1 informative here because the fact that 2 Microsoft pursued this case very aggressively 3 did not request this motion shows at least that 4 they did not believe in good faith that there 5 are grounds to dismiss at this stage of the 6 arbitration. 7 A related point I'd like to raise is that 8 under the AAA Consumer Arbitration Rules under 9 Rule 33, it appears that only dispositive 10 motions can be trialed if a moving party 11 actually makes the request, so I think it's 12 just another point to raise at the outset. 13 Now, on to the second point regarding 14 claimant's contract claims, now both Microsoft 15 and claimant agree on the standard. There 16 needs to be a contract between the parties. 17 There needs to be allegations that Microsoft 18 breached the contract and claimant must show 19 that he suffered damages as a result of the 20 defendant's breach. The parties do not 21 disagree on the standard. The only 22 disagreement was on how the facts actually 23 applied to that standard. Again, at this stage 24 of the case, the facts must be presumed in 25 claimant's favor.</p>	<p style="text-align: right;">Page 13</p> <p>1 wrong with his computer due to the faulty 2 Windows update. Now, these were not just 3 people he found on the street. These are IT 4 professionals with years of experience, have 5 years of working with Microsoft Windows. It's 6 my understanding that actually may even be 7 certified Microsoft technicians. So, the fact 8 that no one claimant reached out to could 9 actually recuperate his documents showed that 10 this was a faulty update. 11 It's important to recognize, Your Honor, 12 that what happened here was not just that 13 Microsoft Windows update caused plaintiff's -- 14 or claimant's computer to crash, the Windows 15 faulty update actually locked plaintiff from 16 getting access to his files. There's an 17 analogy here that I think might be helpful. If 18 you went to a bank and had a safe deposit box 19 and part of the key to the box was a finger ID 20 system where you use your fingerprint. Now, 21 let's say the software for that finger ID 22 system failed, and then it needs to be 23 reinstalled, and all of a sudden that 24 reinstallation loses your actual fingerprint. 25 In that instance, would it make sense to allow</p>

<p style="text-align: right;">Page 14</p> <p>1 the person who had their valuables in that 2 lockbox to not gain access because all of a 3 sudden the computer lost access to their 4 fingerprint? That's precisely what's happening 5 here. Claimant was denied access to get his 6 files ultimately, which were ultimately 7 destroyed, because of this faulty Windows 8 update. 9 Again, looking at what claimant must show 10 at this early stage of the case and what he's 11 actually shown, it's clear that there's enough 12 here to have this case move on to discovery. 13 Now, as to Microsoft's point with respect 14 to precise provisions that need to be 15 identified, those may not have been identified 16 in the amended claim, but they clearly exist 17 and we've outlined in our response to their 18 motion here. 19 Lastly, I'll move on to the negligence 20 claims here. Again, the parties don't dispute 21 what the standard is. The parties just dispute 22 whether or not plaintiff has made the 23 appropriate allegations. But, again, at this 24 early stage of the case, claimant's allegations 25 must be presumed to be true. He states in the</p>	<p style="text-align: right;">Page 16</p> <p>1 with claimant was with respect to Windows 2 update. It wasn't with respect to the tens of 3 thousands of files that were his personal 4 files. 5 Now, in their briefs they mention this one 6 case about a refrigerator, and the refrigerator 7 broke down, and the person lost their food that 8 was in the refrigerator. That's very different 9 than what's happened here. Claimant's files 10 were actually deteriorated where he couldn't 11 actually gain access to files or no longer use 12 them, he literally was blocked from going to 13 them. Again, we don't think that's a fair 14 analogy and think that the other cases that we 15 highlight in our brief are more appropriate. 16 Now, finally, with respect to the 17 amendment, it's also important to recognize, 18 Your Honor, that the claimant was litigating 19 this case pro se for nearly a year when -- 20 JUDGE DERMAN: Excuse me. Isn't he an 21 attorney, Mr. Deutsch? 22 MR. PARASIDIS: He is an attorney but he's 23 not one with experience in litigation, but he 24 is an attorney, yes, Your Honor, but he still 25 was pro se.</p>
<p style="text-align: right;">Page 15</p> <p>1 fourth amended claim that Microsoft had a duty 2 to engage in reasonable conduct in providing 3 its Windows updates. Microsoft breached that 4 duty because it provided a faulty Windows 5 update that was a direct cause, and a cause in 6 fact approximate cause of his harm, and that 7 there was damages, not just to him losing his 8 Windows update on his computer or software -- 9 I'm sorry -- but also losing -- destroying, as 10 we mentioned, all of his files and being 11 precluded from accessing his files, which of 12 course comes back to his One Drive back up, 13 which Microsoft had and still refuses to give 14 him. 15 Now, with respect to the economic loss 16 doctrine, here there clearly are exceptions 17 that New Jersey recognizes and claimant fell 18 squarely within those exceptions. One clear 19 example was a case that we mentioned on our 20 brief where if to the extent that there is 21 supplemental or ancillary damages that were not 22 part of the contract that was bargained for, 23 that falls outside the economic loss doctrine, 24 and here that's exactly what claimant's files 25 are. The contract that Microsoft entered into</p>	<p style="text-align: right;">Page 17</p> <p>1 I'm sure Your Honor and the parties saw 2 earlier on, the filings weren't maybe as well 3 written as you would've seen from an 4 experienced litigator. 5 Now, when the firm took over -- 6 JUDGE DERMAN: Let me ask you a question. 7 What number complaint were you -- amended 8 complaint were you responsible for? 9 MR. PARASIDIS: I was just going to go 10 into that, Your Honor. 11 When the firm came in, we filed the second 12 amended complaint or claim. Right after we 13 filed it, Microsoft asked the law firm to 14 remove one or two statements that were in the 15 claim. We didn't oppose that and we actually 16 did so. And rather than call that change a 17 corrected second amended claim, we just called 18 it a third amended claim just for the sake of 19 simplicity because we think it's hard to follow 20 when you say corrected on the same amended 21 claim. There was the initial amended claim 22 when we first got this case. There was the 23 second amended claim, which we call the third 24 amended claim which Microsoft actually asked 25 for.</p>

5 (Pages 14 - 17)

<p style="text-align: right;">Page 18</p> <p>1 Then, the most recent, the fourth amended 2 claim, the only thing we added there was when 3 we received limited discovery that actually 4 showed that Mr. Deutsch did not use One Drive 5 from the time that Microsoft alleged he did. 6 That was a material fact that we needed to 7 update the pleadings in order to reflect what 8 was revealed in discovery. It's not as if 9 claimant is just throwing things at wall and 10 trying to have them stick. He's being very 11 diligent in his amendment and only bringing 12 them up at the time that they're necessary. 13 There's been absolutely no discovery, no 14 meaningful discovery with respect to these 15 Window 10 claims. And, again, at this stage, 16 we just think it's time to allow at least some 17 discovery to go forward. 18 Thank you, Your Honor. 19 MS. NAHABET: May I speak? 20 JUDGE DERMAN: Sure. 21 MS. NAHABET: First, with regard to the 22 early stages and the argument that Microsoft 23 didn't request authority, I mentioned before 24 that Mr. Stern had made that request and that 25 based off of the fact that Mr. Deutsch was</p>	<p style="text-align: right;">Page 20</p> <p>1 of provisions in the agreement, but none of 2 those provisions are ones in which he has a 3 viable breach of contract claim. And even -- 4 he mentioned something about reaching out to 5 Microsoft themselves, again, that's the first 6 time that we're hearing about that. I'm not 7 aware of Mr. Deutsch having reached out to 8 Microsoft to address his Windows 10 issues and 9 the only time he reached out was with regards 10 to the One Drive, but again it hasn't been 11 alleged before. 12 So, Mr. Parisidis didn't even address the 13 arguments we made with regard to those other 14 provisions. 15 Finally, with regard to negligence, again, 16 Mr. Deutsch has not identified an independent 17 duty outside of the contract that the parties 18 have agreed to. It's really just the fact that 19 the economic laws doctrine applies and the 20 terms of that contract and the terms of that 21 say with regard to those damages it's not 22 limited to just software damages, it includes 23 lost profits, it contemplates lost profits and 24 consequential damages, and other damages as 25 well.</p>
<p style="text-align: right;">Page 19</p> <p>1 proceeding pro se, we first ended up with his 2 motion for preliminary relief and then he 3 considered what was going on before counsel got 4 involved, so we continued on with discovery 5 before making our second request for -- 6 JUDGE DERMAN: You're cutting out. 7 MS. NAHABET: So, I was basically making 8 the point that we had made this request early 9 on as to all claims, not just the Section 230 10 claims. But just because of the way the case 11 progressed, we were working on the Section 230 12 claim because that was Mr. Deutsch's main 13 focus. 14 Moving on to the contracts, while they 15 have identified the support page as in the 16 fourth amended claim, because of the 17 integration clause in the contract that does 18 not fall within the terms of the agreement 19 between the parties and so it is irrelevant and 20 inapplicable. And then, Mr. Parisidis started 21 making some new arguments and allegations. But 22 really what matter is that he hasn't identified 23 the provisions of the contract that are valid 24 that Mr. Deutsch can properly and sufficiently 25 base a claim on. Yes, he identified a couple</p>	<p style="text-align: right;">Page 21</p> <p>1 With regard to this argument about the 2 various amendments, since his firm has been 3 retained, there has been two substantive 4 amendments and this opposition essentially 5 operates as a third amendment. Even with that 6 third amendment, it's not clear how Mr. Deutsch 7 would be able to set forth a viable claim. 8 For those reason, we ask that the 9 remaining claims be dismissed with prejudice 10 and without the opportunity to amend. 11 JUDGE DERMAN: What do you say to 12 Mr. Parisidis's comment that only a party can 13 request a dispositive motion. I guess by way 14 of background, in your original motion, you 15 requested dismissal of the entire complaint, 16 yet you only focused on I would say 80 percent 17 of the claim. And I did raise that issue and 18 then I did give the claimant time to respond. 19 But in hindsight or retrospect, I decided that 20 not sufficient time was available for the 21 claimant to articulate his position. 22 When we had our hearing, notwithstanding 23 the fact that I asked for summary briefs 24 quickly, I did not address those issues, and 25 those outstanding claims, you know, were --</p>

6 (Pages 18 - 21)

<p style="text-align: right;">Page 22</p> <p>1 existed to live to see another day. I</p> <p>2 carefully -- I specifically remember this --</p> <p>3 went through the complaint to see what was</p> <p>4 still viable because as you know there were</p> <p>5 other multiple claims that were dismissed such</p> <p>6 as I believe conversion and consumer fraud.</p> <p>7 And I carefully went through the fourth amended</p> <p>8 complaint to see what still lives and found the</p> <p>9 breach of I guess what we're now calling the</p> <p>10 EULA and the negligence claim.</p> <p>11 So, what do you say, Ms. Nahabet, to his</p> <p>12 comment that you never asked -- I think he's</p> <p>13 implying that I have unilaterally asked for</p> <p>14 this, but what's your response to that?</p> <p>15 MS. NAHABET: Originally, at the very</p> <p>16 start of the case before his firm was retained,</p> <p>17 we did make a request to make a dispositive</p> <p>18 motion briefing with regard to all claims.</p> <p>19 With regard to the more recent request that</p> <p>20 that motion be heard sooner rather than later,</p> <p>21 I think maybe on our end we were just under the</p> <p>22 impression it was limited to this argument</p> <p>23 because we were moving it up, so if we</p> <p>24 inadvertently left it off, then I apologize for</p> <p>25 that, but we had made that request at the very</p>	<p style="text-align: right;">Page 24</p> <p>1 becomes clear that what is at issue here are</p> <p>2 factual interpretations of whether enough has</p> <p>3 been provided here.</p> <p>4 The last point I'd like to make is that</p> <p>5 Microsoft keeps saying that claimant has</p> <p>6 disavowed certain theories and has failed to</p> <p>7 address them and that's just not true.</p> <p>8 Claimant was given only 5 pages to respond to</p> <p>9 this dispositive motion. We didn't have enough</p> <p>10 space to address every single case and every</p> <p>11 single point that was raised.</p> <p>12 To the extent anything has been left off,</p> <p>13 we're happy to address those points right now.</p> <p>14 JUDGE DERMAN: Based on the font that you</p> <p>15 used, that you probably got at least 10 pages.</p> <p>16 MR. SHAPIRO: This is Mark Shapiro.</p> <p>17 Looking at the consumer arbitration, I</p> <p>18 don't think anything precludes Your Honor from</p> <p>19 considering a motion. It says the arbitrator</p> <p>20 may consider a party's request, but nothing</p> <p>21 precludes you from deciding that you want to</p> <p>22 receive such a motion. As Ms. Nahabet said, we</p> <p>23 originally made the request, Mr. Deutsch was</p> <p>24 operating pro se, I think that The Court, Your</p> <p>25 Honor, decided that out of an abundance of</p>
<p style="text-align: right;">Page 23</p> <p>1 start of our case to have dispositive motion</p> <p>2 briefing as to all of the claims in the</p> <p>3 complaint.</p> <p>4 MR. PARASIDIS: May I respond?</p> <p>5 JUDGE DERMAN: Yes. Mr. Parisidis, I</p> <p>6 didn't mean to cut you off. I'd like you to</p> <p>7 have a chance to respond to anything if you'd</p> <p>8 like.</p> <p>9 MR. PARASIDIS: Thank you, Your Honor.</p> <p>10 If Microsoft made a request to dismiss the</p> <p>11 Windows 10 claim, that request clearly was not</p> <p>12 granted because there were no filings on that.</p> <p>13 The fact that it happened before our firm</p> <p>14 joined, I think is immaterial to whether or not</p> <p>15 that request was subsequently made or whether</p> <p>16 or not this was sua sponte motion.</p> <p>17 The second point I'd like to make is that</p> <p>18 we're not at trial here. We're really at an</p> <p>19 early stage of this case. The level of detail</p> <p>20 that Microsoft is basically asserting that this</p> <p>21 claimant's responsibility goes far beyond that</p> <p>22 required by law at this early stage of the</p> <p>23 case. Again, we're on a motion to dismiss.</p> <p>24 Facts must be presumed in claimant's favor and</p> <p>25 as we go more and more into this hearing it</p>	<p style="text-align: right;">Page 25</p> <p>1 caution you would proceed with discovery in</p> <p>2 that context recognizing that he was proceeding</p> <p>3 pro se. If we're going to get hung up on</p> <p>4 formalities and whether we made the motion, or</p> <p>5 didn't make the motion, and what the timing</p> <p>6 was, then we will orally make the motion right</p> <p>7 now, or we can go ahead and make a motion in</p> <p>8 the written format, and then resubmit these</p> <p>9 papers. I think we're getting worked up about</p> <p>10 a formalistic issue that really shouldn't drive</p> <p>11 any of this.</p> <p>12 Just in response to Mr. Parisidis's point</p> <p>13 about this being an early stage, as Your Honor</p> <p>14 knows and you're a sitting state court judge,</p> <p>15 contract claims are routinely dismissed at the</p> <p>16 motion to dismiss stage. It is black letter</p> <p>17 New Jersey law that a party has to allege the</p> <p>18 existence of a contract, has to allege the</p> <p>19 existence of a provision that was breached. As</p> <p>20 Ms. Nahabet said, they certainly didn't allege</p> <p>21 that in their amended complaint. Now, in their</p> <p>22 opposition, they've identified a few</p> <p>23 provisions. They can't get out the gate</p> <p>24 because even the provisions they identified is</p> <p>25 not even plausible that Microsoft could've</p>

7 (Pages 22 - 25)

<p style="text-align: right;">Page 26</p> <p>1 breached for all the reasons that she already 2 laid out.</p> <p>3 We submit, Your Honor, the fact that it's 4 an early stage is not relevant in the context 5 of this breach of contract claim given the 6 inadequacy of the pleadings.</p> <p>7 MR. PARASIDIS: Just one quick point I'll 8 make on that which is that it's one thing to 9 say it's a breach of contract may be grounds 10 for dismissal, it's another to say that the 11 negligence claim would as well and at the very 12 least the negligence claim is far stronger. We 13 think both claims have merit, but the 14 negligence claim is far stronger particularly 15 at this stage of the case.</p> <p>16 MR. SHAPIRO: But not to belabor the 17 point, but obviously we believe there is no 18 negligence claim. All of the parties -- all of 19 the issues here are governed by the contract. 20 They haven't identified anything outside of the 21 contract that would provide a separate 22 independent duty as Ms. Nahabet said. 23 Everything we're talking about, software, 24 functionality of the software, all of it is 25 that's what the EULA is about. If we're not</p>	<p style="text-align: right;">Page 28</p> <p>1 claimant paid for One Drive, signed up for One 2 Drive, paying the services of One Drive solely 3 for this contingency that in the event this 4 computer gets dropped in a bucket or water, the 5 software goes dead, he has this back up. When 6 he called to get the actual back up, the one 7 time in his left that he needed it, Microsoft 8 refused to provide it and continues to this day 9 to refuse to provide the update even though 10 they have all the files.</p> <p>11 JUDGE DERMAN: I understand that if he had 12 had his One Drive, the failure of the software 13 would not have been a problem. I guess my 14 question is did he attempt to update his 15 software because he lost his access on his 16 data on the One Drive? Is there any connection 17 between what happened with his One Drive and 18 his loss in connection and then his attempt to 19 update his computer?</p> <p>20 MR. PARASIDIS: I see, Your Honor. I 21 believe it's the other way around. I believe 22 it's that the computer crashed because of the 23 faulty Windows software. The claimant then 24 went and tried to get his documents from One 25 Drive and then was denied access which he</p>
<p style="text-align: right;">Page 27</p> <p>1 talking about what the parties' relationship is 2 after the purchase and the EULA, then I don't 3 know what we're talking about. It's exactly 4 what the EULA is designed to deal with is what 5 happens with the parties in the event that any 6 issues arise. And certainly, it contemplates 7 those sorts of issues as Ms. Nahabet said, you 8 know, going forward, the warranty extends for a 9 year, we're well past that. Clearly, what the 10 EULA was driving at and is driving at is the 11 relationship between the parties in the event 12 there's any issues with the software and that's 13 exactly what this case is about, it's issues 14 with the software, so the EULA governs this 15 dispute and there is no breach.</p> <p>16 JUDGE DERMAN: Mr. Parisidis, I want to 17 ask you a very basic question. What is the 18 relationship of the One Drive shut down to your 19 client's attempt to do the customary Microsoft 20 update?</p> <p>21 MR. PARASIDIS: My understanding, Judge, 22 is that the relationship between the One Drive 23 shut down and this Windows 10 update is that 24 Windows -- the faulty Windows 10 update 25 basically wiped his computer clean. And</p>	<p style="text-align: right;">Page 29</p> <p>1 claims --</p> <p>2 JUDGE DERMAN: I jotted down -- so I may 3 be wrong -- I jotted down that the One Drive 4 shut down was in the spring of 2020 and then I 5 jotted down again -- it may be wrong -- that 6 the interaction let's say with the IT people to 7 try and correct the problem and eliminate the 8 blue death thing, the blue spiral of death 9 thing my grandson calls it that too, was in 10 June of 2020? Am I wrong that the One Drive 11 shut down preceded the crash?</p> <p>12 MS. NAHABET: That is correct, Your Honor. 13 I believe it was May 2020 when the One Drive 14 was suspended and then June or July when the 15 Windows update happened.</p> <p>16 JUDGE DERMAN: All right, so I guess my 17 question is, you know, did one thing make him 18 do the other because he had lost access to his 19 data or was he doing just a routine perfunctory 20 update and then the computer crashed?</p> <p>21 MR. PARASIDIS: I think it was the latter, 22 Your Honor. I think it was a mandatory update 23 that Microsoft requires all users, you know, 24 whatever they send out -- I don't use 25 Microsoft, but it's whatever they send out</p>

<p style="text-align: right;">Page 30</p> <p>1 periodically.</p> <p>2 JUDGE DERMAN: Right, when they remind you</p> <p>3 do you want to do it now, or tonight, that kind</p> <p>4 of thing?</p> <p>5 MR. PARASIDIS: Exactly.</p> <p>6 JUDGE DERMAN: Again, so his inability to</p> <p>7 access his material on One Drive had nothing do</p> <p>8 with his attempting a mandatory update in the</p> <p>9 software? It would've -- would this have</p> <p>10 happened in any event?</p> <p>11 MR. PARASIDIS: I believe that's right,</p> <p>12 Your Honor. In a sense, I think what you're</p> <p>13 getting at is that they're independent, right?</p> <p>14 So, if his computer crashing, was it caused by</p> <p>15 the faulty Windows update, his lack of access</p> <p>16 to One Drive was due as we alleged in the claim</p> <p>17 Microsoft wrongly flagging him for that</p> <p>18 inappropriate image but it happened more or</p> <p>19 less within a very short time period of one</p> <p>20 another.</p> <p>21 JUDGE DERMAN: Now, does anybody know the</p> <p>22 EULA Exhibit 1 or Exhibit 2, did anybody</p> <p>23 have -- do you know we know whether it's</p> <p>24 Exhibit 1 or Exhibit 2? I think that's a</p> <p>25 manufacturer -- is it Exhibit 1 I believe or</p>	<p style="text-align: right;">Page 32</p> <p>1 relates to the specific provisions that we've</p> <p>2 discussed here.</p> <p>3 JUDGE DERMAN: Well, both sides have done</p> <p>4 a good job for me in identifying the relevant</p> <p>5 provisions in each agreement. I thought maybe</p> <p>6 in the interim you had learned which one it</p> <p>7 was, that's all, okay.</p> <p>8 It's interesting, we have the case about</p> <p>9 the refrigerator and so on and then we have the</p> <p>10 case also that the claimant relies upon, the 2J</p> <p>11 Corporation versus Tice case. I notice it's a</p> <p>12 1997 case. Are there no cases in this -- that</p> <p>13 deal with other property in the context of</p> <p>14 technology? I mean so much has happened in</p> <p>15 technology since 1997 since last week even.</p> <p>16 So, you weren't able to find any cases? I</p> <p>17 guess you would've cited them, Mr. Parisidis or</p> <p>18 Mr. Shapiro, that deal with the data files</p> <p>19 document other property? Nobody found a case?</p> <p>20 MS. NAHABET: Your Honor, I don't believe</p> <p>21 I saw any cases with regard to technology. The</p> <p>22 2J Corp. case is under Pennsylvania law as</p> <p>23 opposed to the Merritt Logan case which was</p> <p>24 decided under New Jersey law.</p> <p>25 MR. PARASIDIS: I will also note that we</p>
<p style="text-align: right;">Page 31</p> <p>1 Exhibit 2 is for retailer? Does anybody know?</p> <p>2 I could have that backwards.</p> <p>3 MS. NAHABET: Let me double check.</p> <p>4 Exhibit 1 is the retailer one and Exhibit 2 is</p> <p>5 the manufacturer one.</p> <p>6 JUDGE DERMAN: I thought I had that</p> <p>7 backwards.</p> <p>8 Do we know which one was used by</p> <p>9 Mr. Deutsch?</p> <p>10 MS. NAHABET: Microsoft doesn't, Your</p> <p>11 Honor. Mr. Deutsch hasn't identified which one</p> <p>12 he's raised, but there are two different EULAs.</p> <p>13 Various answers ago, I think in response to the</p> <p>14 first amended complaint even in the second one,</p> <p>15 but he hasn't identified which one is the</p> <p>16 contract to govern.</p> <p>17 MR. PARASIDIS: I'm not sure there's a</p> <p>18 material change or any difference between the</p> <p>19 two.</p> <p>20 Microsoft, can you point to any material</p> <p>21 difference between the two?</p> <p>22 MS. NAHABET: I mean neither of it relates</p> <p>23 to the claimant in this arbitration, but there</p> <p>24 are differences in terms of how you acquire the</p> <p>25 software and who you go to but not as it</p>	<p style="text-align: right;">Page 33</p> <p>1 did not find any technology related cases but</p> <p>2 the Third Circuit case of 2J Corp. Again, the</p> <p>3 standard there is very clear that the content</p> <p>4 is separate from the holder of the content.</p> <p>5 MR. SHAPIRO: I think the absence of it is</p> <p>6 probably indicative of what is self-evident</p> <p>7 from the EULA itself, that is that in this</p> <p>8 context --</p> <p>9 JUDGE DERMAN: What case did you say?</p> <p>10 MR. SHAPIRO: No, I'm not referencing a</p> <p>11 case. I'm saying the absence of a case is</p> <p>12 likely indicative of the self-evident nature of</p> <p>13 the EULA that is as Ms. Nahabet says the EULA</p> <p>14 says who parties should go to, the differences</p> <p>15 between the two, who parties should go to. I</p> <p>16 think it's self-evident that these type of</p> <p>17 contracts don't necessarily cover the types of</p> <p>18 the issues that we're talking about here, and</p> <p>19 so the absence of cases is probably indicative</p> <p>20 of the fact that when parties bring these</p> <p>21 claims, they're bringing a breach of contract</p> <p>22 claim and it's clear that there is no tort</p> <p>23 claim outside of the contract.</p> <p>24 MR. PARASIDIS: The only point, Judge, I'd</p> <p>25 like to make in response to that, I think that</p>


<p style="text-align: right;">Page 34</p> <p>1 these contracts are always contracts of</p> <p>2 adhesion. They always have these class action</p> <p>3 waivers. They always limit liability. The</p> <p>4 damages are existent but they're not</p> <p>5 astronomical and I think lawyers tend to not</p> <p>6 bring these cases just because there's no money</p> <p>7 there. I wouldn't take the absence of cases to</p> <p>8 mean that there isn't the ability to bring a</p> <p>9 negligence claim.</p> <p>10 MS. NAHABET: Your Honor, I just want to</p> <p>11 add one point --</p> <p>12 JUDGE DERMAN: Yes.</p> <p>13 MS. NAHABET: -- about the Merritt Logan</p> <p>14 case.</p> <p>15 That case does discuss how these types of</p> <p>16 contracts contemplate the price for the sale of</p> <p>17 the item as well. If you're saying if --</p> <p>18 Mr. Parisidis's claimant is arguing that</p> <p>19 Microsoft should be separately liable for</p> <p>20 damage outside of data and that is outside of</p> <p>21 the contract realm, then that doesn't take into</p> <p>22 consideration the fact that Microsoft based the</p> <p>23 price of the software on the terms of this</p> <p>24 agreement and the terms of this sale which</p> <p>25 covers that data as well, any potential</p>	<p style="text-align: right;">Page 36</p> <p>1 CERTIFICATION</p> <p>2</p> <p>3 I, ESTAMARIE CASTELLI-VELEZ, a Shorthand</p> <p>4 Reporter and Notary Public within and for the State</p> <p>5 of New York, do hereby certify the foregoing to be a</p> <p>6 true and accurate transcript to the best of my</p> <p>7 knowledge and ability.</p> <p>8 I further certify that I am not related to</p> <p>9 any of the parties to this action by blood or by</p> <p>10 marriage and that I am in no way interested in the</p> <p>11 outcome of this matter.</p> <p>12</p> <p>13</p> <p>14  ESTAMARIE CASTELLI-VELEZ</p> <p>15</p> <p>16</p> <p>17</p> <p>18</p> <p>19</p> <p>20</p> <p>21</p> <p>22</p> <p>23</p> <p>24</p> <p>25</p>
<p style="text-align: right;">Page 35</p> <p>1 damages, consequential damages, lost profits,</p> <p>2 et cetera. And the Merritt Logan case very</p> <p>3 clearly goes through the contract whereas I</p> <p>4 don't believe the 2J Corp. case does. Again,</p> <p>5 we mentioned the distinction between one being</p> <p>6 under Pennsylvania law and the other being</p> <p>7 under New Jersey law, which is what we're</p> <p>8 dealing with here.</p> <p>9 JUDGE DERMAN: Does anybody else have</p> <p>10 anything else they want to say?</p> <p>11 Okay, so, Counsel, you'll be getting the</p> <p>12 transcript, and then you can get it to me, and</p> <p>13 I'll be writing an opinion on this. It may</p> <p>14 take a while, I'm quite busy, and it's the</p> <p>15 holidays, but I will be writing an opinion.</p> <p>16 MR. PARASIDIS: Thank you, Judge.</p> <p>17 JUDGE DERMAN: Everybody, have a good</p> <p>18 holiday and stay safe.</p> <p>19 And to the court reporter, thank you very</p> <p>20 much.</p> <p>21 (Time noted: 4:44 p.m.)</p> <p>22</p> <p>23</p> <p>24</p> <p>25</p>	

EXHIBIT 32



AMERICAN
ARBITRATION
ASSOCIATION®

INTERNATIONAL CENTRE
FOR DISPUTE RESOLUTION®

Northeast Case Management Center
1301 Atwood Avenue
Suite 211N
Johnston, RI 02919
Telephone: (866)293-4053
Fax: (866)644-0234

February 8, 2022

Jason Lampert, Esq.
Salzano, Lampert & Wilson, LLP
275 Madison Avenue, 35th Floor
New York, NY 10016
Via Email to: jlampert@slwlawoffices.com

Natalie Nahabet, Esq.
Orrick, Herrington & Sutcliffe
777 South Figueroa Street, Suite 3200
Los Angeles, CA 90017
Via Email to: nnahabet@orrick.com

Case Number: **01-20-0014-3715**

Thomas Deutsch, Esq.

-vs-

Microsoft Corporation

Dear Parties:

Enclosed please find **Dismissal Order** from Arbitrator Derman. This order shall continue in effect unless and until amended by subsequent order of the arbitrator.

Formal correspondence regarding case closure will be sent separately.

Sincerely,

/s/

Jenna Pascale
Manager of ADR Services
Direct Dial: (401)406-7095
Email: jennapascale@adr.org

Supervisor Information: Sara Faulkingham, FaulkinghamS@adr.org

Enclosures

bcc:

Hon. Harriet Derman, J.S.C. (ret)

cc:

Frank Salzano, Esq.
Brady Williamson
Marc Shapiro
Efthimios Parasidis

AMERICAN ARBITRATION ASSOCIATION

In the Matter of the Arbitration Between:)	
)	Case No. 01-20-0014-3715
Thomas Deutsch, Esq. (Claimant))	
)	
v.)	
)	
Microsoft Corporation (Respondent))	

**ORDER GRANTING MICROSOFT'S MOTION TO DISMISS OR FOR JUDGMENT
ON THE PLEADINGS ON CLAIMANT'S WINDOWS 10 BREACH OF CONTRACT
AND WINDOWS 10 NEGLIGENCE CLAIMS**

Having considered both Parties' briefing, supporting documentation and oral arguments on December 1, 2021;

IT IS ON THIS 7th DAY OF FEBRUARY, 2022 HEREBY ORDERED AS FOLLOWS:

1. Claimant's Windows 10 EULA breach of contract claim, as set forth in Section F of Count 2 of the Fourth Amended Claim, is here **DISMISSED WITH PREJUDICE**;
2. Claimant's Windows 10 negligence claim, as set forth in Section E of Count 4 of the Fourth Amended claim, is hereby **DISMISSED WITH PREJUDICE**;
3. Claimant's application to amend his Fourth Amended Claim is hereby **DENIED**; and
4. All Counts now having been **DISMISSED WITH PREJUDICE**, the entire matter is hereby **DISMISSED WITH PREJUDICE**.

Harriet Derman

*The Honorable Derman, J.S.C. (Ret.)
Arbitrator*

EXHIBIT 33

From: AAA Jenna Pascale <JennaPascale@adr.org>
Sent: Thursday, February 10, 2022 6:10 AM
To: Harriet Derman; AAA Jenna Pascale
Cc: Nahabet, Natalie; Efthimios Parasidis; cc: Frank Salzano; Jason Lampert; Brady Williamson; Shapiro, Marc R.
Subject: RE: Thomas Deutsch, Esq. v. Microsoft Corporation - Case 01-20-0014-3715
Attachments: 2022-02-07 Memorandum Decision on MTD.pdf
Importance: High

Good Morning Parties:

Attached please find Arbitrator Derman's Memorandum Decision on the Motion to Dismiss.

Thank you,
Jenna Pascale



AAA Jenna Pascale
Manager of ADR Services

American Arbitration Association

1301 Atwood Ave, Suite 211N, Johnston, RI 02919
T: 401 406 7095
adr.org | icdr.org | aaamediation.org

Adam Shoneck, Assistant Vice President
Northeast Case Management Center



The information in this transmittal (including attachments, if any) is privileged and/or confidential and is intended only for the recipient(s) listed above. Any review, use, disclosure, distribution or copying of this transmittal is prohibited except by or on behalf of the intended recipient. If you have received this transmittal in error, please notify me immediately by reply email and destroy all copies of the transmittal. Thank you.

From: Harriet Derman <hderman@newjerseylaw.net>
Sent: Tuesday, February 8, 2022 9:03 AM
To: AAA Jenna Pascale <JennaPascale@adr.org>
Cc: Nahabet, Natalie <nnahabet@orrick.com>; Efthimios Parasidis <eparasidis@slwlawoffices.com>; cc: Frank Salzano <fsalzano@slwlawoffices.com>; Jason Lampert <jlampert@slwlawoffices.com>; Brady Williamson <bwilliamson@slwlawoffices.com>; Shapiro, Marc R. <mrshapiro@orrick.com>
Subject: Re: Thomas Deutsch, Esq. v. Microsoft Corporation - Case 01-20-0014-3715

***** External E-Mail – Use Caution *****

Dear Counsel,
An opinion will shortly follow. Judge Derman

On Tue, Feb 8, 2022 at 8:25 AM <jennapascale@adr.org> wrote:

Hello,

Please review the attached correspondence regarding the above-referenced case.

Feel free to contact me with any questions, comments or concerns you have related to this matter.

Thank you.

[Logo]

AAA Jenna Pascale
Manager of ADR Services
American Arbitration Association

1301 Atwood Ave, Suite 211N, Johnston, RI 02919

T: 401 406 7095

[adr.org](https://www.adr.org)<<https://www.adr.org>> | [icdr.org](https://www.icdr.org)<<https://www.icdr.org>> | [aaamediation.org](https://www.aaamediation.org)<<https://www.aaamediation.org>>

Adam Shoneck, Assistant Vice President
Northeast Case Management Center
[cid:image3c2900.PNG@57b25532.47aca0dd]

The information in this transmittal (including attachments, if any) is privileged and/or confidential and is intended only for the recipient(s) listed above. Any review, use, disclosure, distribution or copying of this transmittal is prohibited except by or on behalf of the intended recipient. If you have received this transmittal in error, please notify me immediately by reply email and destroy all copies of the transmittal. Thank you.

AMERICAN ARBITRATION ASSOCIATION

In the Matter of the Arbitration Between:)	Case No. 01-20-0014-3715
)	
Thomas Deutsch, Esq. (Claimant))	MEMORANDUM DECISION ON
)	DEFENDANT’S MOTION
v.)	TO DISMISS
)	
Microsoft Corporation (Respondent))	

This memorandum represents the Arbitrator’s opinion with respect to the Motion to Dismiss or Motion for Judgment on the Pleadings brought by Respondent Microsoft Corporation (“Microsoft”).

I. PROCEDURAL HISTORY

Claimant Thomas Deutsch, Esq. (“Deutsch”) filed an arbitration with the American Arbitration Association (“AAA”) on August 17, 2020. Microsoft responded on September 15, 2020. Claimant made an application for emergent relief to access his files, but was denied such relief by the first Arbitrator without prejudice on October 22, 2020. Deutsch made an additional application to the undersigned successor Arbitrator on January 14, 2021 for the same emergent relief, but it was denied. Claimant has amended his Claim four times.¹ Some discovery was undertaken between the parties and they entered a Protective Order.

Pursuant to the Scheduling Orders of both February 24, 2021 (after Deutsch was represented by counsel) and May 7, 2021, and pursuant to the authority of Rule 33 of AAA Consumer Arbitration Rules, Microsoft requested and was granted permission to file a dispositive motion.

¹ Before Claimant was represented by counsel, Deutsch, an attorney, amended his Complaint. After he was represented by counsel in early February 2020, counsel amended Deutsch’s Complaint three times (Second, Third, and Fourth) although the Third Amended Complaint was necessitated by the inclusion of language in the Second Amended Complaint, which Microsoft had found unacceptable and counsel for the Claimant agreed to remove.

Microsoft then brought a motion to dismiss or for judgment on the pleadings, essentially with respect to claims impacted by Section 230(c) of the Communications Decency Act, 47 U.S.C. § 230(c). The Arbitrator granted that motion, but did not address the balance of the claims of Claimant, which are Part F of Count II and Count Part E of Count IV² of Deutsch's Fourth Amended Complaint ("FAC"). The Arbitrator set forth her opinion at great length on the record and same was memorialized in an Order dated August 23, 2021, dismissing all claims except those dealing with an alleged malfunction of Windows 10, which Claimant insists caused him to lose certain files.³ The Arbitrator denied Deutsch's request to amend his Complaint for the fifth time. Microsoft has now brought this Motion to Dismiss or for Judgment on the Pleadings for the balance of Claimant's extant claims and Claimant again seeks to amend his Complaint.

II. BACKGROUND

In the Spring of 2020, Claimant learned that his OneDrive account licensed by Microsoft had been suspended when Microsoft claimed it had detected an image containing Child Sexual Exploitation and Abuse Imagery ("CSEAI"). OneDrive is a cloud-storage service that allows the users to store files. The Microsoft Services Agreement controlled the relationship between the parties. As a result of this suspension, Claimant was unable to access his documents on OneDrive. Claimant has always denied the image was CSEAI.

Claimant also claimed that Microsoft failed to warn him that his computer lacked storage space for updates and, without the warning, upon utilizing the update, his computer crashed.

III. STANDARD FOR DISMISSAL.

A motion for judgment on the pleadings is evaluated under the same standards as a motion to dismiss for failure to state a claim upon which relief can be granted. Wolfigton v. Reconstructive Orthopaedic Associates, 935 F.3d 187, 195 (3d Cir. 2019). The motion is cognizable after a party has answered the complaint. See Pressler, Comment 4.1.1 to R. 4:6-2.

² Since it appeared Microsoft was seeking a total dismissal in its moving papers, the Arbitrator asked the parties to address all the claims on short notice, but the Arbitrator did not consider nor hear those additional matters and, indeed, ruled that they survived.

³ The Arbitrator carefully reviewed and modified the Order submitted by Microsoft. Claimant never objected to the form of Order signed on August 23, 2021.

Facts and inferences presented in the pleadings must be viewed in “the light most favorable to the nonmoving party.” Id. (quoting In re Asbestos Prods. Liab. Litig. (No. VI), 822 F.3d 125, 133 n. 6 (3d Cir. 2016)). The motion should be granted if the moving party proves “there are no material issues of fact, and he is entitled to judgment as a matter of law.” Zimmerman v. Corbett, 873 F.3d 414, 417 (3d Cir. 2017) (quoting Sikirica v. Nationwide Ins. Co., 416 F.3d 214, 220 (3d Cir. 2005)). The motion must also be evaluated “in light of the legal sufficiency of the facts alleged in the complaint.” Donato v. Moldow, 374 N.J. Super 475, 482 (App.Div. 2005).

The complaint must be dismissed if it does not articulate a legal basis entitling plaintiff to relief. Camden County Energy Recovery Assocs., L.P. v. New Jersey Dep’t of Env’tl. Prot., 320 N.J. Super 59, 64 (App. Div. 1999). The plaintiff is not obligated to “prove the case but only to make allegations, which, if proven, would constitute a valid cause of action.” Leon v. Rite Aid Corp., 340 N.J. Super 462, 472 (App.Div. 2001). “Factual allegations must be enough to raise a right to relief above the speculative level.” Bell Atlantic Corp. v. Twombly, 550 U.S. 544 (2007). The assertions in a complaint must be sufficient “to state a claim to relief that is plausible on its face,” Id. at 570, so that the court can “draw the reasonable inference that the defendant is liable for the conduct alleged.” Ashcroft v. Iqbal, 556 U.S. 662, 678 (2009). “Threadbare recitals of the elements of a cause of action, supported by mere conclusory statements,” Ashcroft, supra, 556 U.S. at 663, will not suffice. Although “plaintiffs are entitled to every reasonable inference of fact,” Printing Mart-Morristown v. Sharp Elecs. Corp., 116 N.J. 739, 768 (1989), they may not rely on conclusory allegations, hoping that discovery will assist them in finding a cause of action. Id.

R-33 of the AAA Consumer Arbitration Rules provides for the filing of dispositive motions.⁴

⁴ The Rule reads, “The arbitrator may allow the filing of a dispositive motion if the arbitrator determines that the moving party has shown substantial cause that the motion is likely to succeed and dispose of or narrow the issues in the case.” At oral argument, Claimant argued that “Microsoft did not request to file this motion to dismiss,” Transcript 10: 23, but, as previously indicated, Microsoft did make such request and two Scheduling Orders signed by the Arbitrator contemplated the filing of dispositive motions. See Orders dated February 24, 2021 and May 7, 2021.

IV. PARTIES' POSITIONS

A. Claimant's Position

Claimant brings a breach of contract claim with respect to his use of the Windows 10 operating system. He alleges that Microsoft breached the end user license agreement ("EULA"). Deutsch also alleges that Microsoft breached its duty with respect to "mandating and providing Windows 10 updates." Claimant's Opposition to Respondent's Motion to Dismiss or for Judgment on the Pleadings on Claimant's Windows 10 Breach of Contract and Negligence Claims ("Claimant's Opposition") at 3. Additionally, Deutsch claims that when he attempted to update his Microsoft software, he was not warned that his computer lacked sufficient memory to install the update. The installation continued although his Solid State Drive ("SSD") did not have sufficient memory. As a result, his computer "crashed" into the "Blue Screen of Death," eliminating access to his operating system and his computer's contents. When he reinstalled Windows 10, all of his existing documents, data, applications and backups on his SSD drive were erased. According to Claimant, Respondent is responsible for this "economic and other harm." FAC at 12.

Claimant also maintains that the economic loss doctrine, see Section VI A, infra, which prevents a tort recovery when a contractual recovery is appropriate and which doctrine Microsoft invokes, does not prevent his recovery because Microsoft owed him an independent duty not covered by the contract. In addition, his damages emanate from "other property, which was not the subject of, nor the benefit to be received by plaintiff from, the contract at issue." Claimant's Opposition at 4.

B. Respondent's Position

Respondent insists that Claimant's contract claim fails because he does not allege a specific contractual breach. Respondent Microsoft Corporation's Motion to Dismiss or for Judgment on the Pleadings on Claimant's Windows 10 Breach of Contract and Negligence Claims ("Respondent's Motion to Dismiss") at 1. The economic loss doctrine also bars

Claimant's recovery because he bases his recovery under both causes of action, negligence and contract, on the same facts and "he does not identify a duty independent of the EULA that Microsoft owed to him...." Id.

V. COUNT II PART F of CLAIMANT'S FAC

A. Unidentified Breached Contract Provisions

In Part F of Count II of Claimant's breach of contract claim in the FAC, Deutsch alleges that "Microsoft breached the EULA Because it Provided Defective Windows Software Update Process." FAC at 8. He alleged that "Microsoft guarantees that it will provide Microsoft Windows updates that will terminate if a person's computer does not have sufficient memory to fully download the update." Id. He claims that Microsoft's policy was "clear" that if there were not enough space on an internal drive, Microsoft would provide a message to licensees, warning that the Windows update requires more space. "... [W]hen Claimant attempted to install a routine Microsoft Windows 10 update, his SSD hard drive did not have sufficient memory to install the update." Id. The update did not pause and did not alert Claimant to the lack of memory space. "As a direct result of Microsoft's 10 update flaw, Windows crashed into the Blue Screen of Death, which eliminated Claimant's access to the operating system and his computer contents." Id. When Claimant reinstalled Windows 10, all of his applications, documents, data, and backups on his SSD drive were erased. Id.

To establish a breach of contract claim under New Jersey law,⁵ a plaintiff has the burden to show that the parties entered into a valid contract, that the defendant failed to perform its obligations under the contract and, as a result, the plaintiff sustained damages. Coyle v. Englander's, 199 N.J.Super 212, 223 (App. Div. 1985). Claimant agrees. FAC at 6; Opposition Brief at 1-2. A claimant must identify the provision of a contract that is breached. In Eprotec Pres., Inc. v. Engineered Materials, Inc., CIV. 10-15097 DRD, 2011 WL 867542, at **22-23 (D.N.J. Mar. 9, 2011), the court stated, "[u]nder New Jersey law, a complaint alleging breach of

⁵ Both versions of the EULA, attached to Respondent's Motion to Dismiss as Exhibit 1 ¶12 and Exhibit 2 ¶11, provide that the laws of the state or county where the licensee resides applies. Mr. Deutsch is a resident of New Jersey and therefore New Jersey law applies. Reference to New Jersey law was made in Scheduling Order No. 1, dated February 24, 2021. All references hereinafter will be to these Exhibits unless otherwise indicated.

contract must, at a minimum, identify the contracts and provisions breached." The absence of an allegation as to the specific provisions of the contract which was breached is grounds for dismissal. Skypala v. Mortgage Electronic Registration Systems, Inc., 655 F.Supp.2d 451, 459 (D.N.J. 2009) (dismissing claim where "the Complaint does not identify the provisions Plaintiff asserts were breached"). See also McFarlane v. Southern Jersey Family Medical Centers, Inc., No. A-0380-19, 2021 N.J. Super. Unpub. LEXIS 1950 (App. Div. Aug. 30, 2021) (matter dismissed after judge could not identify which provision of the employment agreement plaintiff failed to perform.); Khorchid v. 7-Eleven, Inc., Civil Action No. 18-8525 (JBS/JS), 2018 U.S. Dist. LEXIS 180609 (D.N.J. Oct. 22, 2018) (where court held the plaintiff failed to state a claim under New Jersey law and could not survive a motion to dismiss since it did not adequately identify which contract provision was implicated); See also In re Facebook Internet Tracking Litig., 290 F. Supp. 3d 916, 918 (N.D. Cal. 2017), aff'd in part, rev'd in part and remanded sub nom. In Re Facebook, Inc. Internet Tracking Litig., 956 F.3d 589 (9th Cir. 2020) (no incorporation of documents saved plaintiff's otherwise unidentified contract claim).

Deutsch's FAC does not recite any provision of either version of the EULA that was violated by Microsoft. Claimant in his FAC referred to Microsoft's technical support page, FAC at 8, n. 6. He insisted that Microsoft guaranteed that Microsoft Windows updates will terminate if a user's computer does not have adequate memory to absorb the update. Id. at 8. These support pages, however, not incorporated into the EULA, do not establish enforceable promises between the parties.⁶ Both forms of the EULA include an integration clause:

Entire Agreement. This agreement (together with the printed paper license terms or other terms accompanying any software supplements, updates, and services that are provided by the device manufacturer or installer, or Microsoft, and that you use), and the terms contained in web links listed in this agreement are the entire agreement for the software and any such supplements, updates, and services (unless the device manufacturer or installer, or Microsoft, provides other terms with such supplements, updates, or services).

Exhibit 1 ¶ 15. (emphasis in original).

⁶ If the Microsoft technical support page were incorporated into the EULA, that agreement's limitation on liability, Exhibit 1 ¶ 9 and Exhibit 2 ¶ 13-16, would confine his relief to repair, replacement or refund of the Windows 10 software.

Exhibit 2 ¶14 has similar language. The web links do not include the support page upon which Claimant relies.

A contract may include reference to other documents, but only if the contract makes clear reference to the document and describes it in such terms that its identity may be ascertained beyond doubt. York Mech. Corp. v. Kinney Cons. Servs., Inc., No-A-4654-18, 2021 WL 829929, at *3 (App.Div. Mar. 18, 2021)(Williston on Contracts § 30:25 (Lord ed. 1999)). The parties to a contract may incorporate contractual terms by reference to a separate, non-contemporaneous document....” Id., but only if the party “had knowledge of and assented to the incorporated terms.” Alpert, Goldberg, Butler, Norton & Weiss, P.C. v. Quinn, 410 N.J.Super. 510, 533 (App.Div. 2009).

The support page is not referenced in the EULA and therefore cannot be included as part of the terms of the EULA and the focus of any breach. See also In re Facebook Internet Tracking Litig., supra, 290 F. Supp.3d at 920 (“[T]he Court finds that the Data Use Policy was not incorporated by reference into the SRR [Statement of Rights and Responsibilities] because the SRR did not ‘clearly and unequivocally’ reference it.”); Ward v. TheLadders.com, Inc., 3 F. Supp. 3d 151, 163 (S.D.N.Y. 2014) (“Thus, plaintiffs’ assertion that the representations elsewhere on the website were part of the Terms of Use is deficient and without merit, and therefore, no claim for breach of contract can be based on these representations.”); (Woods v. Google Inc., No. 05:11-cv-1263-JF, 2011 U.S. Dist. LEXIS 88795 (N.D. Cal. Aug. 10, 2011) (“At least as they are described in the current complaint, the terms of the invalid click policy are not articulated adequately to be deemed incorporated into the Agreement”).

The New Jersey Supreme Court has spoken clearly on this subject. “The essence of voluntary integration is the intentional reduction of the act to a single memorial; and where such is the case (sic) the law deems the writing to be the sole and indisputable repository of the intention of the parties.” Harker v. McKissock, 12 N.J. 310, 321-22 (1953). The integration clause in either version of the EULA bars Claimant’s attempt to rely on other, non-contractual provisions as the basis of his breach of contract claims.

Claimant, however, attempted to assert the relevant breaches of contract in his Opposition to the Motion to Dismiss. See Claimant’s Opposition at 2. Such effort will not spare

the Claimant. Car Carriers, Inc. v. Ford Motor Co., 745 F.2d 1101, 1107 (7th Cir. 1984), cert. denied, 470 U.S. 1054, 1758 (1984) (“It is axiomatic that the complaint may not be amended by the briefs in opposition to a motion to dismiss.”). See also Penn. ex rel. Zimmerman v. PepsiCo, Inc., 836 F.2d 173, 181 (3d Cir. 1988).

Even if this attempt at amending the complaint in Claimant’s Opposition were sustainable and giving every “reasonable presumption in the plaintiff’s favor,” Car Carriers, Inc., supra, 745 F.2d at 1107, the allegations of breach in the EULA⁷ do not rescue Claimant’s Claim. In his opposition, Deutsch claims that “by providing a faulty update that caused Claimant’s operating system to generate the Blue Screen of Death,” Microsoft has breached the EULA provisions with regard to updates and caused him to sustain damages.⁸ Claimant cites, without more, to Exhibit 1 ¶ 6 and to Exhibit 2 ¶ 6⁹ of Respondent’s Motion. He also cites without explication to “related warranties” and references Exhibit 1 ¶ 9 and Exhibit 2 at 13-16. Finally, Claimant alleges that Microsoft breached the EULA provisions which are applicable to support procedures for updates. Exhibit 1 ¶ 10 and Exhibit 2 ¶ 9.

The only contractual undertaking in Exhibit 1 ¶ 6 and Exhibit 2 ¶ 6 is that of the Claimant, who as indicated, agreed to receive automatic updates without any additional notice. Microsoft made no undertaking in this Section.

Reference to the warranty provisions of Exhibit 1 § 9 and Exhibit 2 § 13-16 does not establish a cause of action for breach. Exhibit 1 ¶ 9 provides for a limited warranty commencing “when the first user acquires the software, and lasts for one year if acquired from Microsoft, or for 90 days if acquired from a device manufacturer or installer.” Claimant acquired the software “sometime not long after August 16, 2017.” See Reply Brief, Exhibit 1, Answer to Interrogatory #2. The alleged conduct occurred in June 2020. Exhibit 2 provides the same limitation.

⁷ According to the Respondent, there are two versions of the EULA which could apply in this matter: There is “one that applies when a customer buys Windows 10 from a device manufacturer or a software installer (the ‘OEM’ version); (sic) and one for purchases from Microsoft or a retailer (the ‘retailer’ version).” Exhibit 1 and Exhibit 2.

⁸ Claimant described his damages as follows: “the technical and legal costs incurred to attempt to regain access to his files, and subsequent loss of the documents, data, and programs therein.” Opposition Brief at 2-3. Additionally, Deutsch described that he sustained “harms (sic) to his personal and professional life.” Opposition Brief at 3 (citing FAC at 21).

⁹ Both Exhibit 1 ¶ 6 and Exhibit 2 ¶ 6 read as follows: “The software periodically (sic) checks for system and app updates, and downloads and installs them for you. You may obtain updates only from Microsoft or authorized sources, and Microsoft may need to update your system to provide you with those updates. By accepting this agreement, you agree to receive these types of automatic updates without any additional notice.”

Reliance on Exhibit 1 ¶ 10 and to Exhibit 2 ¶ 9 is also unavailing because the language of both provisions is only informative about how support can be obtained and makes no commitments.¹⁰ Microsoft has no affirmative obligation under the update provision. Deutsch invokes Microsoft's "guarantee," FAC at 8, but does not cite to a guarantee provision. Additionally, Claimant did not acquire support from Microsoft. According to the FAC, Deutsch utilized the services of third-party technicians. FAC at 3.

Claimant has not identified a specific provision of the EULA that was breached by Microsoft; this omission is fatal to his contract claim.

B. Warranty Limitations

Even if there were a contract provision that were relevant, Claimant confronts barriers to his case in the comprehensive provisions under the various warranty sections. Exhibit 1 ¶ 9 disclaims all implied warranties and section c provides under the Limited Remedy section that if there were a breach of the limited warranty, the remedy is limited to (i) repair or replacement of the software at no charge to the consumer¹¹ or (ii) accept return of the software for a refund of the amount paid. **"These are your only remedies for breach of warranty."** (emphasis in original). Exhibit 2 at 13 has the same language.

Section d, Damages, is also specific as to the limitation on damages: **"Except for any repair, replacement, or refund that Microsoft, or the device manufacturer or installer, (sic) may provide, you may not under this limited warranty, under any other part of this agreement, or under any theory, recover any damages or other remedy, including lost profits or direct, consequential, special, indirect, or incidental damages."** (emphasis in original). Exhibit 2 Limited Warranty Section (¶¶13-16) has the same limiting language.

Claimant is barred from any financial recovery by these provisions.

¹⁰ Exhibit 1 § 10 reads: **"Support. a. For software preinstalled on a device.** For the software generally, contact the device manufacturer or installer for support options. Refer to the support number provided with the software. For updates and supplements obtained directly from Microsoft, Microsoft may provide limited support services for properly licensed software as described at (aka.ms/support). **b. For software acquired from a retailer.** Microsoft provides limited support services for properly licensed software as described at (aka.ms/ms/support)." Exhibit 2 ¶ 9 has similar language. (emphasis in original).

¹¹ This limitation on damages in the EULA would preclude any recovery beyond "repair, replacement, or refund" of the Windows 10 software so that the implications of the Arbitrator's ruling on §230 would not be avoided.

C. Contract of Adhesion

At oral argument and in his FAC, Deutsch asserted the provisions of limited liability and warranty constitute a contract of adhesion and should not be enforced.

As Claimant argues in his FAC at 14-15, while contracts are generally enforced as written, Vasquez v. Glassboro Serv. Ass’n Inc., 83 N.J. 86 (1980), New Jersey courts do not hesitate to strike limited liability clauses that are unconscionable or violative of public policy. Moreira Constr. Co., Inc. v. Moretrench Corp., 97 N.J.Super. 391, 394 (App. Div. 1967), aff’d, 51 N.J. 405 (1968). While “[t]here is no hard and fast definition of unconscionability,” Lucier v. Williams, 366 N.J.Super. 485, 492 (App. Div. 2004), “... the Supreme Court explained in Kugler v. Romain, 58 N.J. 522 (1971), unconscionability is “an amorphous concept obviously designed to establish a broad business ethic.” Lucier, supra, 366 N.J.Super at 492 (citing Kugler, supra, 58 N.J. at 543). A lack of “good faith, honesty in fact and observance of fair dealing” is involved. Id. at 544. The court looks not only at the adhesive nature of the contract, Lucier, supra, 366 N.J. Super at 492, but also to “the subject matter of the contract, the parties’ relative bargaining positions, the degree of economic compulsion motivating the ‘adhering’ party, and the public interests affected by the contract.” Id. (citing Rudbart v. North Jersey District Water Supply Comm’n, 127 N.J. 344, 356, cert. denied, 506 U.S. 871 (1992)). With limitation of liability issues, a court focuses on bargaining power, the status of the parties and the substance of the contract. Lucier, supra, 366 N.J. Super at 492.

The court also analyzes whether “the limitation is a reasonable allocation of risk between the parties or whether it runs afoul of the public policy disfavoring clauses which effectively immunize parties from liability for their own negligent actions.” Id. (citing Valhal Corp. v. Sullivan Assoc., Inc. 44 F.3d 195, 202-204 (3d Cir. 1995)).

With these principals in mind, the case of D’Agostino v. Appliances Buy Phone, Inc., 2016 N.J.Super. LEXIS 504 (App.Div. Mar. 8, 2016), cited by Respondent, is instructive. Plaintiff, an electronics engineer and computer scientist, brought a claim against his client, Appliances Buy Phone, for whom he provided website development, and against Google. Google, in the exercise of its policy of removing duplicate sites, barred a site plaintiff had enrolled in the Google Merchant Center on behalf of the client. After reaching out to Google, plaintiff was allowed to have his site participate in Google Product Search. In the meantime, he became

embroiled in a dispute with his client and his client claimed that Google was forcing it to shut down one of the apparently duplicate sites. Although Google reapproved plaintiff's account, he was unable to access the website which the client had shut down. This was the website that generated consulting fees for the plaintiff. Plaintiff sued his client and Google. His claim against Google dealt with its temporary suspension of access to his website.

The judge granted summary judgment to Google on plaintiff's breach of contract and implied covenant of good faith and fair dealing claims. He reviewed the language of the Terms of Service agreement ("TOS") and found that the contract was not an adhesion contract and that the exculpatory clauses were enforceable. These provisions, similar to the provisions in the EULA, disclaimed warranties and limited damages. The trial court, citing Hoffman v. Supplements Togo Management, LLC, 419 N.J.Super 596 (App.Div. 2011), certif. granted, 209 N.J. 231 (2012), found that "the website was not designed in a manner that makes it unlikely that consumers would even see it at all on their computer screens." The trial judge also found that the TOS warned a user that it had a right to terminate or suspend access to Google services. In addition, Google acted reasonably to suspend the account when it identified two companies with similar names, selling the same products at the same price in contravention of its policies. When Google discovered that the websites were not duplicates, plaintiff's website was restored with access to the Google Product Search service. The trial court did not find a contract of adhesion.

The Appellate Division reviewed the decisions as to whether the TOS was a contract of adhesion and whether the contract's exculpatory clauses were enforceable.

As to the contract of adhesion issue, the court described "the take-it-or-leave-it" basis used in standardized printed forms without the opportunity for negotiation. Id. at 41. Such contracts may be unenforceable "if the terms are manifestly unfair or oppressive and are dictated by a dominant party." Id. at 42 (citing Howard v. Diolosa, 241 N.J.Super 222, 230 (App. Div.), certif. denied, 122 N.J. 414 (1990)). Invariably, these are aspects of procedural unconscionability so that a fact-sensitive examination of substantive unconscionability is required. Id. Gross disparity in bargaining power may be obvious from the contract itself. Id. If the disparity is not self-evident, both procedural unconscionability, focusing on the process by

which the contract is entered, and substantive unconscionability, focusing on the existence of one-sided terms, must be considered. Id. at 42.

The Appellate Division noted that an exculpatory clause is only enforceable if “(1) it does not adversely affect the public interest; (2) the exculpated party is not under a legal duty to perform; (3) it does not involve a public utility or common carrier; or (4) the contract does not grow out of unequal bargaining power or is otherwise unconscionable.” Id. (quoting Gerson v. Regency Driving Ctr., Inc., 368 N.J.Super 237, 247 (App. Div. 2004)). Full knowledge of the consequences must be understood when a party gives up his or her legal rights. Id.

Unlike the trial court, the Appellate Division found that the TOS was a contract of adhesion because of the take-it-or-leave-it nature of the relationship. The plaintiff was not free to negotiate the terms. Id. Nevertheless, it did not find that the TOS was unenforceable, relying on Martindale v. Sandvik, Inc., 173 N.J. 76, 90 (2002), which focused on “the degree of economic compulsion motivating the adhering party” and the public interests affected by the contract. With these standards in mind, the Appellate Division found that the TOS was neither procedurally nor substantively unconscionable. Plaintiff was a sophisticated webmaster who understood “click wrap” contracts, such as the TOS. He was not under any economic compulsion as there were alternative shopping services. And there was no public interest at stake. Id. The disclaimer of warranties and the limitation of liability clause satisfied the Gerson factors.

The same analysis applies to Claimant. While Deutsch is not a website designer or a computer scientist, he is an attorney with graduate degrees. The subject of the controversy is a software license for windows operating systems. Some familiarity with computers is necessary. Claimant knew how to articulate his problem with OneDrive when he first filed, by himself, his claim against Microsoft with AAA in August 2020. In the FAC, he acknowledged that Deutsch wanted Microsoft OneDrive “to ensure his documents, data and backups were always available to him in the cloud.” FAC at 1. Claimant made full use of the potential of Windows 10:

After subscribing and immediately transferring all of his documents, data and backups onto OneDrive, Claimant spent a great deal of time reorganizing Claimant’s files on OneDrive as well a continuing to add and modify documents, data and

backups. Claimant used One Drive as a cloud backup for all of his documents, data and backups for his personal Dell desktop computer at his residence (the “Desktop”) and the Photos folder on his iPhone.

Id.

Claimant indicated he has “two hard drives in his Desktop; one is a solid state hard drive (The ‘SSD’) that allows for faster processing of programs, the other is a ‘regular’ hard drive that has slower processing speeds, but much larger storage capacity.” Id. at 2.

Deutsch is hardly a novice computer user, availing himself of a computer with hesitancy for only personal email or to search the Internet. His licensing and use of Microsoft’s products reveal that he was familiar with and knowledgeable about computers, operating systems, software, storage, and backup products.

Additionally, there is no concern with regard to a consumer victimized by the contractual provisions. Microsoft consumers have other options. There was no economic “compulsion” as plaintiff could have purchased a different operating system or licensed alternative software. “Although Microsoft overwhelmingly dominates the PC operating-systems market, other operating systems exist.” Novell, Inc. v. Microsoft Corp., 505 F.3d 302, 305 (4th Cir. 2007). See Lucier, supra, 366 at 488 (the court was concerned that many homebuyers in New Jersey would have no recourse if a home inspector failed to act diligently). No public interest is implicated if the EULA is enforced.

There is nothing in the record that indicates the disclaimer of warranties and the limitation on liability were in a miniscule font, designed to be unread or unnoticed. No perfunctory “click” entrapped the licensee.

As noted, infra, see Section VIB, the United States Supreme Court has commented that a purchaser pays less for a product when a manufacturer can limit its liability by disclaiming warranties and circumscribing remedies. East River S.S. v. Transamerica Delaval, 476 U.S. 858, 873 (1986).

The Arbitrator finds the disclaimer of warranties and exculpatory clauses are valid and enforceable and, as the Appellate Division stated in D’Agostino, not so “one-sided as to shock the court’s conscience.” D’Agostino, supra, 2016 N.J.Super. LEXIS 504, at *45 (citing Sitogum Holdings, Inc. v. Ropes, 352 N.J.Super 555, 565 (Ch. Div. 2002)).

Claimant, as previously indicated, acquired the software in August 2017 and the problem with the software occurred in June 2020. Respondent Microsoft Corporations' Reply in Support of Motion ("Reply Brief"), Exhibit 1, Claimant's answer to Interrogatory #2. Any warranty expired August 2018. Remedies, such as damages or injunctive relief, are unavailable to Claimant.

D. Causation

While causation is an issue in this case with Respondent claiming that Deutsch's use of third-party non-Microsoft IT technicians to reinstall Windows 10 caused the loss of Claimants' documents and not any action by Microsoft, the Arbitrator need not decide this issue because of the basic deficit of Claimant's contract claim.

E. Summary of Contract Claim

Because Claimant does not identify a provision of the contract that has been breached and because the disclaimer of warranties and limitations on liability is enforceable, Claimant fails to state a claim under New Jersey law. Therefore the Arbitrator grants the motion to dismiss Count II F.

VI. COUNT IV E of CLAIMANT'S FOURTH AMENDED CLAIM

A. Economic Loss

Microsoft moves to dismiss Claimant's Windows 10 negligence cause of action based on the economic loss doctrine. Respondent points out that Deutsch's negligence claim "mirrors the allegations underlying Claimant's breach of contract claim." Reply Brief at 3. And so it does. In Count II F of the FAC at 8, part of the contract allegations, Deutsch refers to the lack of sufficient memory to install the update and Microsoft's failure to provide a warning. In Count IV E, also a surviving count, Deutsch alleges that Microsoft breached its duty by failing "to create Windows 10 updates that auto-stop and create an alert if a user's computer does not have sufficient memory to install the update." FAC at 12.

Claimant argues that his negligence claim is based on Microsoft's express policies. FAC at 8-9.¹² He claims that "Microsoft had a duty to engage in reasonable conduct in mandating and providing Windows 10 updates, that Microsoft breached that duty because the company provided Claimant with a faulty Windows 10 update." Opposition Brief at 3. Claimant has not identified any discrete and distinct duty owed to him by Microsoft, separate and apart from EULA contractual undertakings, which would entitle him to assert an independent negligence claim and entitle him to relief. See FAC at 9, 12-13.

In Saltieri v. GSI Consultants, Inc., 170 N.J. 297 (2002), the seminal New Jersey case on the subject of economic loss, plaintiff, a landscape architect, alleged that the corporate defendant who had entered a contract with plaintiff to design and prepare specifications for the turfgrass on two athletic fields negligently prepared the turfgrass specifications. This failure caused financial loss to the plaintiff. Plaintiff attempted to hold the corporate officers personally liable for allegedly tortious conduct, utilizing the participation theory of liability. The Supreme Court acknowledged that if only contract rules applied rather than tort principles, the participation theory of liability would be unavailable. Id. at 309. Additionally, a tort claim remedy dramatically affects the rules governing damages. Id. at 309.

The Supreme Court discussed the history of contract versus tort through the lens of the common law and New Jersey jurisprudence. It found, "Under New Jersey law, a tort remedy does not arise from a contractual relationship unless the breaching party owes an independent duty imposed by law." Id. at 316 (citing New Mea Construction Corp. v. Harper, 203 N.J.Super. 486, 493-94 (1985) (court declined to hold a builder personally liable for damages resulting from negligent workmanship). The Supreme Court was unable to identify any duty owed to the plaintiff "that is independent of the duties that arose under the contract." It canvassed duties implied by law, such as those imposed upon attorneys and physicians, and found no duty that was specifically imposed by law in New Jersey for the provider of turf design specifications, the alleged tortfeasor in Saltieri.

12. In Claimant's W10 Response, upon which the Arbitrator does not rely, Claimant wrote: "Additionally Microsoft cannot on the one hand argue that Claimant's Window's 10 software claims, premised on Microsoft's own express policies, are not contract claims while on the other hand arguing for the dismissal of Claimant's negligence claim because it 'only flows from a contract.'"

Similarly, there is no duty that can be imposed upon Microsoft, separate and apart from its contractual undertaking.¹³ Any obligation it has to Claimant emanates from a contract paradigm.

B. Support Pages Duty

To avoid being limited to a contractual remedy, however, Deutsch now claims that Microsoft had an independent duty deriving from the support pages. He claims that “Here, Microsoft made representations on their (sic) website – and not contained in the EULA – regarding the Windows 10 software update auto-stopping and alerting a Windows 10 user when the user’s computer did not have sufficient memory to install the update.” Claimant’s Opposition at 4. These representations, according to Claimant, created the duty owed to him as a Windows 10 user and the breach of this duty entitles Claimant to damages.

Viability of the tort claim as opposed to the contract claim “depends on whether the tortious conduct alleged is extrinsic to the contract between the parties.” CapitalPlus Equity, LLC v. Prismatic Dev. Corp., Civil Action No. 07-321 (WHW), 2008 U.S. Dist. LEXIS 54054 at *6 (D.N.J. July 16, 2008). Windows 10 software updates are detailed in the contract. The EULA specifically states as follows:

This agreement applies to the Windows software that is preinstalled on your device, or acquired from a retailer and installed by you, the media on which you received the software (if any), any fonts, icons, images or sound files included with the software, and also any Microsoft updates, upgrades, supplements or services for the software, unless other terms come with them. (emphasis added)

Exhibit 1 ¶ 1.a; Exhibit 2 ¶ 1.a.

There are other references to the software and its performances. See Exhibit 1 ¶9a and Exhibit 2 at 13. (“Depending on how you obtained the Windows software, Microsoft or the device manufacturer or installer, warrants that properly licensed software will perform

¹³ Claimant admitted this in his response submitted on June 25, 2021: “It is undisputed that Microsoft’s software and updates, including Windows 10 update which caused Claimant to experience the well-known Blue Screen of Death and led to his hard drives, files, and programs being permanently erased, is governed by EULA.” Because the Arbitrator decided not to consider the submissions made on short notice, no weight is given to this statement.

substantially as described in any Microsoft materials that accompany the software.”). Finally, the EULA expressly provides that Microsoft does not offer any other express warranties and excludes implied warranties. Exhibit. 1 ¶ 9 B; Exhibit 2 at 13. Therefore any statements with regard to updates on Microsoft’s website are irrelevant because the parties had agreed all such issues would be controlled by the EULA. Hence, an alleged misrepresentation that "involve[s] a nonfulfillment of a warranty or guarantee contained within the contract itself" cannot be said to be extraneous to the contract. Florian Greenhouse, Inc. v. Cardinal IG Corp., 11 F. Supp. 2d 521, 528 (D.N.J. 1998). See also Montclair State Univ. v. Oracle USA, Inc., 20212 U.S. Dist. LEXIS 119509, at *15 (D.N.J. Aug. 23, 2012).

Claimant has identified no separate duty, preventing the application of the economic loss doctrine.

C. Damage to Other Property

Claimant insists that the generalized concept of economic loss recovery restricted to the contract terms is overcome when there is “damage to other property which was not the subject of the contract, nor the benefit to be received by the plaintiff from, the contract at issue.” Opposition Brief at 4. He relies on the case of 2-J Corp. v. Tice, 126 F.3d 539, 542-545 (3d Cir. 1997).

Allocation of economic loss between a manufacturer and a consumer involves assessment of tort and contract principles in the determination of claims arising out of the manufacture, distribution, and sale of defective products. Generally speaking, tort principles are better suited to resolve claims for personal injuries or damage to other property. See Spring Motors Distributors, Inc. v. Ford Motor Co., 98 N.J. 555, 579-80 (1985); East River S.S., *supra*, 476 U.S. at 871-72 (1986); Seely v. White Motor Co., 63 Cal. 2d 9 (1965); Bocre Leasing Corp. v. General Motors Corp., 84 N.Y.2d 685 (1995). Contract principles more readily respond to claims for economic loss caused by damage to the product itself. See Spring Motors, *supra*, 98 N.J. at 580; East River, *supra*, 476 U.S. at 871-72; Seely, *supra*, 45 Cal.Rptr. 17; Lewinter v. Genmar Indus., 26 Cal. App. 4th 1214 (1994); Florida Power & Light Co. v. Westinghouse Elec. Corp., 510 So. 2d 899, 901-02 (Fla.1987); Oceanside At Pine Point v. Peachtree Doors, Inc., 659 A.2d 267, 270 (Me.1995); Bocre Leasing, *supra*, 621 N.Y.S. 2d at 501.

The case of 2-J Corp., emanating from a pre-technology world in 1997, is distinguishable and was derived from the Third Circuit's effort to predict what the Pennsylvania Supreme Court would do if presented with a similar case. In 2-J Corp., plaintiff sought to recover in tort for damage to its inventory stored in a warehouse which collapsed allegedly because of defective manufacturing. In this 1997 case, the Third Circuit reviewed two United States Supreme Court cases for guidance. The first case was E. River S.S. v. Transamerica Delaval, Inc., supra, 476 U.S. 858, where the court held that when the plaintiff, a charter of a super-tanker, sued the manufacturer of the supertanker's turbines in tort, there was no recovery for the product itself. The Supreme Court regarded the injury as the failure of the product to function properly, reflecting "the essence of a warranty action, through which a contracting party can seek to recoup the benefit of its bargain." 2-J Corp., supra, 126 F. 3d at 542 (citing East River S.S., supra, 476 U.S. 867-868).

E. River S.S. includes an excellent discussion on maintaining the distinction for tort recovery for physical injuries and warranty recovery for economic loss:

Damage to a product itself is most naturally understood as a warranty claim. Such damage means simply that the product has not met the customer's expectations, or, in other words, that the customer has received "insufficient product value." The maintenance of product value and quality is precisely the purpose of express and implied warranties. Therefore, a claim of a nonworking product can be brought as a breach-of-warranty action. Or, if the customer prefers, it can reject the product or revoke its acceptance and sue for breach of contract. (citations omitted).

E. River S.S., supra, 476 U.S. at 872.

The United States Supreme Court noted that the purchaser pays less for a product when a manufacturer can restrict its liability, within limits, by disclaiming warranties or limiting remedies. E. River S.S., supra, 476 U.S. at 873. ("In exchange, the purchaser pays less for the product.")

In the second United States Supreme Court, Saratoga Fishing Co. v. J.M. Martinac & Co., 520 U.S. 875 (1997), also a maritime case, the Court found that, after a fire, flooding and sinking as the result of a defective hydraulic system, extra equipment was "other property," which had been added by the initial user so that the second owner could maintain a lawsuit against the

manufacturer. In Saratoga Fishing Co., the Supreme Court found that the fishing equipment foreseeably added to the ship by the initial user did not become a part of the “product itself,” 2-J Corp, supra, 126 F.3d at 544. Therefore inventory foreseeably stored by an initial user did not become integrated into the subject matter of the contract, the warehouse, and a suit could be maintained.

But neither United States Supreme Court case provides support for Claimant and his reliance on 2-J Corp is misplaced.

Reference to the jurisprudence of New Jersey and federal courts sitting in New Jersey, however, is more appropriate. In Spring Motors Distributors, supra, 98 N.J. at 561, when a plaintiff who sold and leased trucks alleged that defects in the transmissions caused it to sustain consequential damages, the New Jersey Supreme Court confined its remedy to breach of warranty under the Uniform Commercial Code (“UCC”) and foreclosed claims in strict liability or negligence.

In Alloway v. General Marine Industries., L.P., 149 N.J. 620 (1997), the court extended the holding of Spring Motors to transactions in goods among non-commercial buyers. It explained the relationship of contract and tort principles:

Tort principles more adequately address the creation of an unreasonable risk of harm when a person or other property sustains accidental or unexpected injury. When, however, a product fails to fulfill a purchaser’s economic expectations, contract principles, particularly as implemented by the U.C.C., provide a more appropriate analytical framework. (citations omitted).

Id. at 628

In In re Merritt Logan, 901 F.2d 349 (3d Cir. 1990), when the buyer of a defective refrigeration system sued the manufacturer, the installer, and the seller for tort claims for damage to the food spoiled when the refrigeration system failed, he was foreclosed from pursuing a remedy: “The damage to Merritt Logan’s food stocks occurred at the core of the commercial transaction.” Id. at 362. The Merritt Logan court predicted that the New Jersey Supreme Court would not accept a limitation on the economic loss doctrine to allow a tort claim for the spoiled food stocks and would instead commit the plaintiff to a recovery

exclusively pursuant to the UCC, which permits consequential damages **unless** the parties have contracted to exclude them. Id. at 363. (emphasis added).

More recent cases in New Jersey have concurred. In Int'l Flavors & Fragrances, Inc. v. McCormick & Co., 575 F. Supp. 2d 654 (D.N.J. 2008), International Flavors & Fragrances (“IFF”) brought suit for breach of express and implied warranties and products liability and fraudulent concealment/legal fraud. McCormick, a wholesale supplier of paprika, allegedly shipped 5,000 pounds of paprika infested with cigarette beetles. Plaintiff had apparently used some of the contaminated paprika in preparing barbeque seasoning. McCormick moved for partial summary judgment on the non-warranty claims. The Honorable Faith S. Hochberg granted the motion and found the economic loss doctrine limits the scope of the product liability claims. The judge anticipated how the New Jersey Supreme Court would rule on the issue of physical damage other than to the product itself. She reviewed Spring Motors and Alloway: “The New Jersey Supreme Court’s analyses in Spring Motors and Alloway generally counsel in favor of limiting IFF to contract remedies.” Id. at 660. The trial judge noted that the several circuits including the Third Circuit’s decision in In re Merritt Logan have “relied on the doctrine to limit the reach of the ‘other property’ exception to the doctrine.” Id. She acknowledged that like the plaintiff IFF in her matter, the plaintiff in Merritt Logan had argued that the defective refrigeration system had caused damaged food stocks, other property, and it could recover either in tort or breach of warranty under New Jersey law, but this position had been rejected by the Third Circuit because the food stocks “occurred at the core of a commercial transaction.” IFF v. McCormick, at 660 (citing Merritt Logan, supra, 901 F.2d at 362). Judge Hochberg adopted that reasoning and found that the “incorporation of the paprika into the barbeque seasoning occurred at the core of a commercial transaction.” Id. at 661.

After perusing decisions from other Districts, Judge Hochberg concluded that if IFF’s position with respect to other property were to prevail, “contract law would drown in a sea of tort.” Id. at 662 (citing East River S.S., supra, 476 U.S. at 866).

In Travelers Indem. Co. v. Dammann & Co., 592 F.Supp. 2d 752 (D.N.J. 2008), another New Jersey case with the same aggrieved party, IFF, a manufacturer of food flavorings, was foreclosed from bringing a products liability claim against Dammann, a producer of raw foods, including vanilla beans, when mercury contamination was found in the beans. Referring to In

Merritt Logan, the District Court found that “IFF’s claims for damages in this action are for damages alleged to have occurred at the core of the commercial transaction with Dammann, i.e., damages from tainted vanilla beans.” Travelers, supra, 592 F.Supp. 2d at 761. The judge would not expand recovery beyond the contract: “When, however, a product fails to fulfill a purchaser’s economic expectations, contract principles, particularly as implemented by the U.C.C., provide a more appropriate analytical framework.” Id. at 761 (citing Alloway, supra, 149 N.J. at 639). The parties’ expectations are relevant. The damage that occurred must be at the core of the parties’ commercial transaction and be contemplated by the parties. Id. at 763. See also Adams Extract & Spice, LLC v. Van De Vries Spice Corp., 2011 u LEXIS 147851, 2011 WL 6756973 *15 (D.N.J. Dec. 23, 2011).

In addition, 2-J Corp., upon which Claimant relies, applies Pennsylvania law while the applicable law in this matter is that of the state of New Jersey. The New Jersey jurisprudence is replete with the refusal of state and federal judges to eschew the application of the economic recovery doctrine as outlined above. 2-J Corp. is also silent as to whether the contract in question had a definitive contract with an exhaustion clause, such as the EULA, which set the parameters and limitations for the parties’ obligations and possible recovery for damages.

Claimant asserts damages with respect to lost data and electronic files and, as a result, failed economic expectation. Such damages are within the contemplation of the sale of the software and implicitly contractual. “When a company agrees to render a service or sell a product, a contract normally will define the scope of the parties’ specific obligations.” Saltieri, supra, 170 N.J. at 316. The relevant sections of the EULA, Exhibit 1 ¶19 and Exhibit 2 at 13, are edifying. They deal with not only “repair, replacement, or refund” of the software, but address, although excluding, direct, consequential, special, indirect, or incidental damages. Furthermore, as noted in E. River S.S., supra, 476 U.S. at 873, the price is positively affected for the purchaser if the manufacturer can restrict its liability.

Deutsch in an attempt to differentiate his loss from any generated by the EULA (and subject to the bar of economic recovery) attempts to narrow the subject of the EULA and confine it to only the licensing of software. Opposition Brief at 5 (“The Sole property subject to, and bargained for, by Claimant as it related to the EULA was the Microsoft Windows 10 software”). To sidestep the impediment of economic recovery, Claimant must identify the

relevant duty and damages that flow from the breach of duty of the Microsoft updates and support pages. Claimant's Opposition at 4. But the updates and software functionality are not extrinsic to the EULA licensing agreement. As previously indicated, the EULA references updates and upgrades. Respondent's Brief, Exhibit. 1 ¶ 1.1a; Exhibit 2 ¶ 1.a. The EULA addresses the performance of the software. Respondent's Brief, Ex. 1 ¶ 9; Exhibit 2 ¶ 13. Any issues with regard to statements on Microsoft's website on updates and software functionality are irrelevant since the parties' agreement is reflected in the EULA exclusively.

Additionally, as previously indicated, the updates and software functionality are not extrinsic to the contract. See Respondent's Brief. Exhibit. 1 ¶1 and Exhibit 2 ¶ 1.a. The damage allegedly sustained by Claimant is at the "core of the transaction" and the transaction involved the licensing of Windows 10. The creation of data and electronic files is the *raison d'être* for the sale of the software.

Finally, 2-J Corp., the case upon Claimant relies, applies to tangible property, the contents of a collapsed warehouse. Files and data stored on a computer through an operating system enabled by software are not in the same category. Counsel for Claimant does not cite to a single case that deals with "other property" in the context of computer technology, operating systems, the Internet, software, cloud storage, etc. to overcome the economic loss impediment.

The files and data lost by the Claimant represent the same damages asserted by him in his breach of contract claim and are central to the transaction for Windows 10.¹⁴ Windows 10 is an operating system.

"An operating system amounts to the computer's core software — software that allows the everyday user to take advantage of a computer's functions. Users often rely on an operating system to open and close other applications — word processors, spreadsheets, calendars, or the like." Novell, Inc. v. Microsoft Corp., 731 F.3d 1064, 1066-67 (10th Cir. 2013). (emphasis added). Software instructions "tell a computer what to do. Software comprises the

¹⁴ Claimant was previously barred from data recovery because of Microsoft's immunity under Section 230. Claimant cannot succeed with a "backdoor" effort through his Windows 10 claim. See Opposition Brief at 2 ("Blue Screen of Death, [which] blocked Claimant's access to his entire set of documents and programs) and FAC at 9 ("[r]einstalling Windows, had the effect of erasing all of Claimant's applications, documents, data and backups on his SSD drive.").

entire set of programs, procedures, and routines associated with the operation of a computer system.” *Encyclopedia Britannica*, 14 Jan. 2021, <https://www.britannica.com/technology/software>

Claimant used the Windows 10 software to enable file management and storage. He claims that Microsoft’s breach of the EULA caused him to lose his “documents, data, and programs,” Opposition Brief at 3. This loss, presumably through the file management and storage feature of Windows 10, is at the core of the transaction. The alleged faulty Windows 10 update deprived Claimant of the opportunity to receive the benefit of file management and storage. These functions are fundamental to the capabilities of Windows 10 and are central to its purpose. They cannot be artificially separated to create a subset of damages that will enable Claimant to secure a tort remedy for “other property.” The files and data are not “other property”; they are the substance, the very core, of the transaction.

D. Summary of Negligence Claim

Claimant’s negligence claim is barred by the economic recovery barrier. His negligence claim is not independent of his contract claim under the EULA.

VII. CLAIMANT’S REQUEST TO AMEND HIS FOURTH AMENDED COMPLAINT

Claimant has requested that he be allowed to amend his Fourth Amended Complaint. The Arbitrator declines to grant such application. While motions to amend are typically granted liberally, and a court may deny leave to amend only when “the moving party has demonstrated undue delay, bad faith or dilatory motives, (2) the amendment would be futile,¹⁵ or (3) the amendment would prejudice the other party.” *Wolfington v. Reconstructive Orthopaedic Associates II PC*, 935 F.3d 187, 210 (3d Cir. 2019) (quoting *United States ex rel. Customs Fraud Investigations, LLC v. Victaulic Co.*, 839 F.3d 242, 249 (3d Cir. 2016)). (emphasis added). “At the same time, a court is justified in denying leave to amend when a plaintiff ‘repeated[ly] fail[s] to cure deficiencies by amendments previously allowed.’” *In re Zoom Video Commc'ns Inc. Privacy Litig.*, 525 F. Supp. 3d 1017, 1028 (N.D. Cal. 2021) (citing *Carvalho v. Equifax Info Servs., LLC*,

¹⁵ If the latitude that Claimant took in setting forth new theories in his Opposition Brief is indicative of what his Fifth Amended Claim would assert, it is clear such efforts would be futile.

629 F.3d 876, 892 (9th Cir. 2010)). A court's discretion to deny leave to amend is particularly broad where plaintiff has previously amended the complaint." Id. (citing Cafasso, U.S. ex rel. v. Gen. Dynamics C4 Sys., Inc., 637 F.3d 1047, 1058 (9th Cir. 2011) (quotation marks omitted)).

Claimant has amended his complaint four times, which means he has had five "bites at the apple." Claimant has had some discovery.¹⁶ See Exhibit 2, Claimant's First Set of Document Requests, and Exhibit 4, Claimant's First Set of Interrogatories, to Respondent's Reply. Claimant alleges that while he did have some discovery, he did not have any discovery on the Windows 10 issue. Opposition Brief at 5. The Scheduling Orders, in accordance with the goals of R-22 of the AAA, seeking efficiency and economy, provided for limited Document Requests and Interrogatories. Claimant made his selection.

Claimant can never overcome the obstacles to his contract claim nor will he be able to overcome the barrier of the economic loss claim. Even if he could, the disclaimer and limited warranties, already expired, bar his recovery.

VIII. CLASS ACTION

Since the entire FAC has now been dismissed, no class action can proceed as the matter is moot. See Dabush v. Mercedes-Benz USA, LLC, 378 N.J. Super. 105 (App. Div. 2005); Hilton Apartments v. Goitein, No. A-0796-18T2, 2020 N.J. Super. Unpub. LEXIS 2145 (Super. Ct., App. Div., Nov. 10, 2020). There are no applicable exceptions. See Richardson v. Bledsoe, 829 F.3d 273, 279 (3d Cir. 2016); Zirger v. Gen. Accident Ins. Co., 144 N.J. 327, 330 (1996) (citing N.J. Div. of Youth & Family Servs. v. J.B., 120 N.J. 112, 119-120 (1990)).

¹⁶ The Arbitrator signed a subpoena to be served upon Verizon Communications, Inc. at the request of Claimant.

IX. CONCLUSION

For the reasons set forth above, Microsoft's Motion to Dismiss is **GRANTED** with respect to Count II F and Count IV G and all Counts now having been **DISMISSED WITH PREJUDICE**, the entire matter is hereby **DISMISSED WITH PREJUDICE**.

Harriet Derman

*The Honorable Derman, J.S.C. (Ret.)
Arbitrator*

DATED: February 7, 2022

Word Doc. #A1416936.docx.hd/bc

EXHIBIT 34

From: Tom Deutsch <tomdeutsch@aol.com>
Sent: Monday, May 9, 2022 2:00 PM
To: Shapiro, Marc R.; Nahabet, Natalie
Cc: tomddeutsch@aol.com
Subject: Thomas Deutsch v Microsoft Motion to Vacate Attached
Attachments: Motion to Vacate 5.9.22.pdf

Marc/Natalie,

Please find attached a Motion to Vacate Arbitrator Derman's Orders, submitted today *pro se* to the Federal District Court for the District of New Jersey in Newark. I have sent a hard copy of the Motion via certified mail today to Marc's New York Office.

I am working on finalizing a retainer agreement with appellate counsel. I expect my counsel to be in touch shortly regarding a stipulated briefing schedule, as well as correcting any *pro se* mistakes, organizing/expanding the Motion as appellate counsel deems appropriate and submitting appropriate documents and exhibits.

Sincerely,

Tom Deutsch

917.406.5648